Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

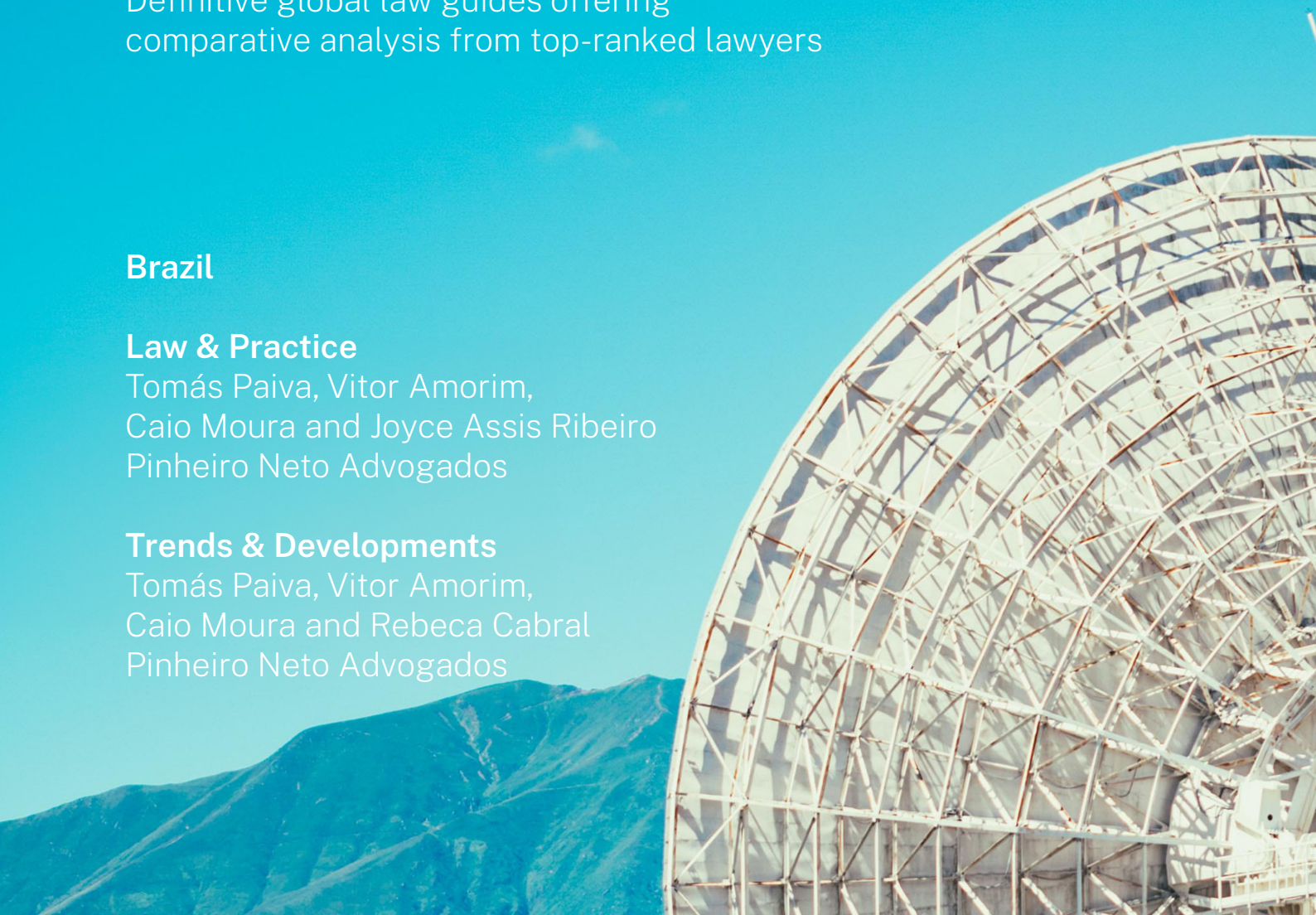
TMT 2026

Definitive global law guides offering comparative analysis from top-ranked lawyers

Brazil

Law & Practice
Tomás Paiva, Vitor Amorim, Caio Moura and Joyce Assis Ribeiro
Pinheiro Neto Advogados

Trends & Developments
Tomás Paiva, Vitor Amorim, Caio Moura and Rebeca Cabral
Pinheiro Neto Advogados



BRAZIL



Law and Practice

Contributed by:
Tomás Paiva, Vitor Amorim, Caio Moura and Joyce Assis Ribeiro
Pinheiro Neto Advogados

Contents

1. Digital Economy p.4
1.1 Legal Framework p.4
1.2 Key Challenges p.5
1.3 Digital Economy Taxation p.5
1.4 Taxation of Digital Advertising p.6
1.5 Consumer Protection p.7
1.6 The Role of Blockchain in the Digital Economy p.7

2. Cloud and Edge Computing p.8
2.1 Highly Regulated Industries and Data Protection p.8

3. Artificial Intelligence p.8
3.1 Liability, Data Protection, IP and Fundamental Rights p.8

4. Internet of Things p.9
4.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.9
4.2 Compliance and Governance p.10
4.3 Data Sharing p.10

5. Audiovisual Media Services p.11
5.1 Requirements and Authorisation Procedures p.11

6. Telecommunications p.12
6.1 Scope of Regulation and Pre-Marketing Requirements p.12
6.2 Net Neutrality Regulations p.13
6.3 Emerging Technologies p.13

7. Challenges With Technology Agreements p.14
7.1 Legal Framework Challenges p.14
7.2 Service Agreements and Interconnection Agreements p.15

8. Trust Services and Digital Entities p.16
8.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.16

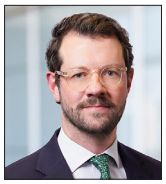
9. Gaming Industry p.17
9.1 Regulations p.17
9.2 Regulatory Bodies p.18
9.3 Intellectual Property p.18

10. Social Media p.20
10.1 Laws and Regulations for Social Media p.20
10.2 Regulatory and Compliance Issues p.21

11. Data Privacy and Cybersecurity p.21
11.1 Data Privacy in Telecommunications p.21
11.2 Cybersecurity in Digital Media and Streaming Services p.23

Pinheiro Neto Advogados has rendered legal services in all legal areas since 1942 and has the structure to offer its clients comprehensive assistance with their business activities. The firm provides services to approximately 2,000 local and international groups, and has offices in São Paulo, Rio de Janeiro, Brasília, Palo Alto and Tokyo. With over eight decades of experience and clients spanning more than 80 countries, the firm has developed a unique, tight-knit culture focused on ever-improving the delivery of legal services in Brazil. Pinheiro Neto Advogados has lawyers specialising in all areas of law.

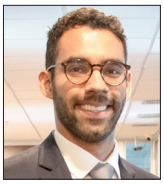
Authors



Tomás Paiva advises Brazilian and international clients on regulatory and contractual matters in the technology, media and telecommunications (TMT) and infrastructure sectors. His practice encompasses regulatory advisory work – including regular engagement with key regulatory authorities such as ANATEL and ANCINE – as well as the structuring and negotiation of complex transactions involving TMT-related products and services. Tomás has extensive experience across a broad range of technologies and regulatory frameworks, having advised on major transactions in the sector, and has built a strong track record in securing regulatory approvals.



Vitor Amorim advises Brazilian and international clients on regulatory, contractual, and transactional matters related to infrastructure and public law, with a particular focus on the technology, media and telecommunications (TMT) sector. He has broad experience across all verticals of the TMT industry, including mobile services, fibre optics, satellites, passive infrastructure, and OTT platforms. Amorim brings a strong transactional focus to his practice, regularly assisting clients in the design and structuring of business models within the sector. He also has an established track record in administrative and judicial litigation and has advised TMT clients on landmark legal disputes.



Caio Moura advises domestic and international clients on litigation, contracts, and regulatory and transactional matters in public law across the technology, media and telecommunications (TMT) and infrastructure sectors. His expertise includes complex and innovative matters involving telecommunications services, radio spectrum use, infrastructure sharing, critical infrastructures, internet applications, new technologies regulation, and the structuring and regulatory approval of complex businesses and transactions.



Joyce Assis Ribeiro advises domestic and international clients on regulatory, transactional and contractual matters in the technology, media and telecommunications (TMT) sectors, with additional focus on entertainment and data protection. Her expertise includes telecommunication services, critical infrastructure, submarine cable systems, data centres, satellite landing rights, internet regulation, and digital platforms. Joyce also represents clients in regulatory proceedings before the National Telecommunications Agency (ANATEL).

Pinheiro Neto Advogados

Rua Hungria, 1100
01455-906
São Paulo
Brazil

Tel: +55 11 3247 8400
Email: tpaiva@pn.com.br
Web: www.pinheironeto.com.br

1. Digital Economy

1.1 Legal Framework

Brazil's digital economy is governed by a robust set of legal and regulatory frameworks that establish ongoing compliance obligations for organisations operating in the country. The key components of this framework include the following.

Core Laws and Regulations (Hard Law)

Brazil's Internet Law (Law No 12,965/2014)

This law sets out fundamental principles for the use of the internet in Brazil, including the following.

- Net neutrality – internet service providers must treat all data, content, and applications equally, with no discrimination or prioritisation of traffic.
- Freedom of expression – users have the right to express opinions and share information online, subject to constitutional and legal limitations.

Decree No 8,771/2016

This decree complements the Internet Law by defining rules for data protection, transparency obligations, and security standards applicable to internet service providers and application providers.

General Data Protection Law (Law No 13,709/2018 – LGPD)

Modelled closely on the EU's GDPR, the LGPD regulates the collection, processing, storage, and sharing of personal data by both public and private entities. It requires a lawful basis for processing (such as consent or legitimate interest) and grants data subjects rights including access, portability, and erasure.

The LGPD applies to any organisation that processes personal data belonging to individuals located in Brazil.

Consumer Protection Code (Law No 8,078/1990)

This foundational consumer rights statute applies fully to digital products and services. It establishes strict liability for defective goods and services and prohibits deceptive or misleading advertising. The law reinforces transparency and fairness across digital commercial practices.

E-Commerce Decree (Decree No 7,962/2013)

This decree sets specific rules for e-commerce, requiring clear and accessible information about products, services, pricing, and supplier identification. It also guarantees the seven day right of regret, allowing consumers to return online purchases unconditionally and receive a full refund.

Industry Codes of Conduct (Self-Regulation)

National Council for Advertising Self Regulation (CONAR)

CONAR establishes the primary standards for advertising practices across all media, including digital platforms. Although participation is voluntary, its decisions carry significant weight, as media outlets and platforms routinely remove advertisements found to be non-compliant.

1.2 Key Challenges

Brazil's Evolving Regulatory Landscape for the Digital Economy

Brazil's regulatory framework for the digital economy is undergoing rapid transformation, driven by assertive judicial decisions and multiple legislative initiatives currently under consideration in Congress. The summary below outlines the key legal developments impacting digital services, digital markets, and content governance.

Platform Liability

Article 19 of Brazil's Internet Law

Brazil is experiencing a significant shift away from its traditional safe-harbour model. Historically, platforms were only liable for user-generated content if they failed to comply with a court-ordered takedown. However, following the Supreme Court's landmark decisions in RE 1.037.396 and RE 1.057.258, Article 19 was deemed partially unconstitutional.

Under the new framework:

- Platforms may incur civil liability without a prior court order if they do not promptly and proactively remove manifestly unlawful content (eg, terrorism, child exploitation, racism, and violence against women).
- Liability also extends to paid or boosted content when platforms financially benefit and harm results.

ANATEL's Regulation on Conformity Assessment and Homologation of Telecommunications Products (Resolution No 780/2025, RACHPT)

ANATEL has recently updated its rules governing the certification and homologation of telecommunications products. A notable change is the introduction of joint and several liability for marketplaces and digital platforms that offer non-certified telecom products.

Regulation on User Duties (in consultation)

ANATEL is currently evaluating new obligations for "large users" of telecommunications services, including Value-Added Service (VAS) and Over-the-Top (OTT) providers. As these entities are legally classified as "users" under the Brazilian Telecommunications Law, the proposal could lead to:

- increased regulatory oversight;
- additional operational and compliance obligations;
- higher transactional costs; and
- potential constraints on innovation.

Content Moderation

Youth Law (Law No 15,2011/2025)

Effective as of 17 March 2026, the Youth Law establishes a comprehensive framework to protect children and adolescents in digital environments. It applies to any digital product or service designed for minors or reasonably likely to be accessed by them.

Key obligations for digital service providers include:

- preventing access to harmful or illegal material (eg, sexual exploitation, violence, and predatory advertising);
- implementing reliable age-verification systems and parental-control tools; and
- publishing compliance reports and appointing a legal representative in Brazil.

MisInfo Bill (Bill of Law No 2,630/2020)

This bill aims to enhance accountability and transparency requirements for social media platforms, search engines, and messaging services with ten million or more users in Brazil, regardless of their corporate headquarters. Its goal is to curb online misinformation through stricter platform-governance obligations.

Market Structure and Competition

Brazilian DMA + DSA (Bill of Law No 2,768/2022)

Often compared to the European Union's Digital Markets Act, this bill targets large digital platforms perceived as holding gatekeeping power. It applies to companies generating at least BRL70 million in annual revenue from Brazilian users and imposes competitive and non-discrimination obligations, irrespective of where the company is headquartered.

1.3 Digital Economy Taxation

In Brazil, digital services and goods are taxed under a dual indirect tax system. Digital services fall under ISS, a municipal tax levied at 2–5% on gross income. Goods and many digital products, however, are often subject to ICMS, a state-level VAT generally applied at 18%, even when the transaction is entirely digital.

Because there is no clear statutory definition separating services from goods, this structure has historically created significant uncertainty and litigation – especially in areas such as cloud computing, SaaS, streaming, and other technology-driven business models.

At the federal level, PIS and COFINS apply to gross income from digital transactions at 3.65% or 9.25%. Cross-border acquisitions of digital services may additionally trigger PIS/COFINS-Importação (commonly 9.25%), CIDE-Technology (10%) and withholding income tax (15–25%, depending on the transaction's characterisation and where the benefit is effectively enjoyed).

Brazil's ongoing tax reform will significantly reshape this landscape. The new dual-VAT system (IBS/CBS) introduces a destination-based consumption tax that replaces the traditional ISS/ICMS split. Under the reformed model, most digital goods and services will receive a unified VAT treatment. This should reduce interpretative disputes but will increase the need for accurate compliance, digital traceability and strong documentation. Although transitional rules extend until 2033, taxpayers must already adapt systems to identify taxable events, determine customer location, and integrate mandatory e-invoicing.

Main Challenges

Brazil's tax environment is characterised by frequent legislative changes, decentralised authorities and complex interactions between federal, state and municipal rules. This results in uncertainty for domestic and multinational businesses alike. Companies must navigate divergent interpretations among tax authorities while managing a heavy volume of ancillary obligations – including e-invoicing, SPED reporting, digital bookkeeping and real-time transactional controls.

Beyond the volume of obligations, taxpayers face sector-specific rules and differing tax treatments for similar activities. The ability to take credits (for ICMS and 9.25% PIS/COFINS) often depends on supplier compliance and proper electronic validation of transactions, making continuous supply-chain monitoring essential.

The tax reform adds another layer of structural challenge. During the transition to the IBS/CBS system, which runs until 2033, taxpayers will need to comply with both the current framework and the new VAT model simultaneously. This will require updating internal systems, managing two sets of reporting requirements, and integrating new digital compliance standards.

In this complex environment, strong tax governance, technology investment and proactive monitoring are critical for businesses seeking to manage risk and maintain compliance.

1.4 Taxation of Digital Advertising

For many years, advertising activities – including digital advertising – faced significant controversy in Brazil due to a longstanding debate over whether they should be taxed as "services" (ISS) or as "communication services" (ICMS). This dispute generated extensive litigation throughout the country. The inclusion of a specific item for advertising services in the statutory ISS list ultimately resolved this jurisdictional conflict, confirming ISS as the appropriate tax for such activities.

Today, the main challenges no longer stem from the ISS/ICMS debate, but from the way digital advertising businesses structure and deliver their products. Different operational models – such as traditional advertising services, platform-based solutions, programmatic advertising, or the licensing of digital tools – may result in distinct tax treatments. As digital advertising increasingly relies on technology, algorithms and data, correctly defining the underlying activity has become essential to ensure proper tax treatment and minimise exposure.

Ensuring Compliance

Compliance in the digital advertising sector begins with accurately characterising transactions and understanding how payments flow. While federal taxes such as PIS and COFINS generally apply across models, the nature of each activity determines whether ISS is due, whether withholding income tax applies and, in cross-border operations, whether PIS/COFINS-Importação and CIDE are triggered. Clear contractual drafting, detailed documentation, and

consistency between contractual terms and actual service delivery are crucial to support the chosen tax characterisation.

Brazil's tax reform adds further complexity. In addition to creating a new VAT system (IBS/CBS), which will gradually replace ISS, ICMS, PIS and COFINS, the reform introduces significant changes to ancillary obligations and to the mechanics of the non-cumulative regime – a system that allows companies to offset VAT paid on inputs against VAT due on outputs. Under the new framework, VAT credits will only be recognised if suppliers comply with e-invoicing rules, accurately report transactions and effectively pay the tax in the preceding stage. For digital advertising companies, these requirements will directly influence pricing, contract terms and platform operations.

Although the transition period extends until 2033, companies should begin preparing now to ensure a smooth and compliant migration to the new system.

1.5 Consumer Protection

In addition to the Consumer Protection Code (Law No 8,078/1990) and the E-Commerce Decree (Decree No 7,962/2013) described in **1.1 Legal Framework**, digital service providers must also comply with the following regulations.

Customer Service Decree (Decree No 11,034/2022)

This decree sets unified customer-service standards across regulated sectors such as telecommunications. It requires providers to offer omnichannel support, comply with maximum waiting times, and ensure that services can be cancelled through the same channel used for contracting. For example, if a customer subscribes to a service through a mobile app, the option to cancel must also be available within the app.

ANATEL's Regulation on Telecommunications Services Consumers' Rights (Resolution No 765/2023)

This regulation outlines the rights of telecommunications service users, with a primary focus on B2C relationships. It may also apply in B2B scenarios when the contracting entity qualifies as a "consumer," meaning it uses the telecom service as the end user.

To comply with these consumer-protection standards, companies should implement strong internal procedures, including staff training, clear policies aligned with applicable regulations, and ongoing monitoring and auditing. These practices help ensure transparency, proper handling of requests, and full adherence to regulatory obligations.

Resolution of Consumer Complaints

Disputes in the digital economy are resolved under the broader consumer-protection framework outlined in **1.1 Legal Framework**. In the telecommunications sector, ANATEL administers specific procedures for handling consumer requests and complaints.

Brazil also provides several government-managed mechanisms for resolving consumer disputes, including the following.

- Consumidor.gov.br – an official online platform that facilitates direct communication between consumers and companies for dispute resolution.
- PROCON (Consumer Protection Agencies) – state-level administrative bodies responsible for enforcing consumer rights and mediating conflicts.
- SENACON (National Consumer Secretariat) – the federal authority responsible for co-ordinating national consumer-protection policy and oversight.

1.6 The Role of Blockchain in the Digital Economy

Brazil's crypto-asset market is governed by Law 14,478/22, in force since June 2023, which establishes a legal and regulatory framework for virtual asset service providers (VASPs). These entities include intermediaries and custodians of virtual assets. The law defines virtual assets to include cryptocurrencies and stablecoins, while excluding instruments such as utility tokens and securities – the latter being regulated by the Brazilian Securities Commission (CVM).

The Central Bank of Brazil, as the financial services regulator, has been granted authority to regulate and supervise VASPs. In November 2025, it issued its first set of rules for VASPs (Resolutions 519 and 520), which became effective on 2 February 2026. These rules provide a 270-day window – until 30 October 2026 – for existing VASPs to apply for licensing.

Banks, foreign-exchange brokers, and securities brokers are also permitted to offer virtual asset services without needing to obtain an additional licence.

Under Communiqué 40,874 (issued 6 November 2023), VASPs may continue operating without prior authorisation until the new rules take effect and throughout the subsequent 270-day application period.

2. Cloud and Edge Computing

2.1 Highly Regulated Industries and Data Protection

Brazil does not have a single, comprehensive statute dedicated specifically to cloud or edge computing. Instead, it regulates these technologies through sector-specific rules.

Government/Public Sector

Normative Instruction No 05/2021 – Office of Institutional Affairs of the Presidency of the Republic

Establishes minimum security requirements for federal agencies adopting cloud solutions. These requirements include data classification, encryption, and formal risk-management processes.

Normative Instruction No 08/2025 – Office of Institutional Affairs

Authorises, under strict conditions, the processing of classified government information in private or community clouds hosted in Brazil by certified providers. The use of public or hybrid clouds remains prohibited, and top-secret data cannot be processed in any cloud environment.

Banking and Finance Sector

Central Bank Resolution No 4,658/2018

Requires financial institutions to implement a cybersecurity policy and sets conditions for contracting cloud services. This includes conducting due diligence on cloud providers and ensuring adequate business-continuity and incident-response procedures.

National Monetary Council Resolution No 4,983/2021

Defines governance rules for outsourcing data processing and storage, including cloud services, whether located in Brazil or abroad.

Telecommunications

ANATEL Cybersecurity Regulation (Resolution No 740/2020)

Requires telecommunications providers to use products and equipment – including cloud services – that comply with cybersecurity policies aligned with the Regulation. Providers must also undergo periodic independent audits.

Processing of Personal Data

All digital infrastructure operators in Brazil must comply with the General Data Protection Law (LGPD), which establishes strict rules for the collection, processing, storage, and transfer of personal data.

Key compliance challenges include cross-border data transfers, data-localisation concerns, and ensuring that companies maintain robust governance and privacy mechanisms.

The Brazilian Data Protection Authority (ANPD) has yet to issue several critical regulations needed for full implementation of the LGPD, including decisions on international data transfers and adequacy rulings for foreign jurisdictions.

On a positive note, most companies operating in Brazil already follow data-protection practices aligned with LGPD principles and international industry standards.

3. Artificial Intelligence

3.1 Liability, Data Protection, IP and Fundamental Rights

AI Laws and Regulations

A comprehensive AI regulatory framework (Bill No 2,338/2023) is currently under review by the House of Representatives, following its approval by the Senate in December 2024. The Bill aims to regulate the development, promotion, and ethical use of AI, establishing principles, accountability mechanisms, individual

rights, governance structures, and risk-based classifications.

Key provisions
- Establishes national guidelines for the development, implementation, and responsible use of AI systems.
- Seeks to protect fundamental rights, ensure safe and reliable AI systems, and promote innovation and competitiveness.
- Combines a principles-based regulatory approach with prescriptive obligations for AI stakeholders.

Sectoral guidelines
Although Brazil does not yet have a unified AI law, several sectors apply AI governance principles.

In telecommunications, AI use must comply with existing legislation and adhere to principles such as reliability, responsibility, non-discrimination, plurality, privacy and data protection, fundamental rights, sustainability, and transparency/explainability. ANATEL is also updating telecom regulations to address AI across the service chain.

Protection of Likeness and Moral Rights, and Deepfakes

Brazil has introduced measures to address the misuse of AI-generated content, especially in electoral contexts.

- TSE Resolution No 23,732/2024: Prohibits AI-generated content – including deepfakes – in electoral propaganda unless it is clearly labelled. Manipulations intended to harm or benefit candidates are strictly banned.

Additional legislative initiatives aim to criminalise malicious deepfake use and protect personality rights.

Law No 15,123/2025

This law amends the Criminal Code to criminalise the creation of non-consensual intimate content using AI. Penalties are increased when the AI-generated content is highly realistic.

4. Internet of Things

4.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Key Laws and Regulations

National IoT Plan (Decree No 9,854/2019)
Brazil's National IoT Plan establishes the country's strategy for developing the IoT ecosystem. It defines IoT as an infrastructure that enables digital services and categorises it as a Value-Added Service, which allows for more flexible and streamlined regulation. The plan directs public investment and regulatory sandboxes toward four priority sectors:

- health;
- agriculture;
- industry 4.0; and
- smart cities.

Tax incentives (Law No 14,108/2020)
To support the commercial viability of IoT solutions, Brazil temporarily removed several telecommunications fees (FISTEL – TFI/TFF) that typically apply to telecom stations. This exemption significantly reduces operational costs for IoT providers and remains in effect until late 2025. Legislative proposals are currently under discussion to extend the incentives and avoid a sudden increase in deployment costs.

Data protection (Law No 13,709/2018 – LGPD)
Brazil's General Data Protection Law applies broadly across sectors but has particular importance within the IoT ecosystem. IoT devices – such as smart home systems, wearables, and urban monitoring technologies – produce large volumes of personal data. As a result, companies operating in this space are subject to strict LGPD compliance requirements and oversight from the national data protection authority (ANPD).

Telecommunications Regulations

Regulatory licensing
To reduce bureaucratic hurdles and facilitate large-scale IoT and M2M deployments, ANATEL recently exempted stations integrated into M2M systems from requiring individual regulatory licensing (MCOM Ordinance No. 17,456/2025).

Cybersecurity and equipment homologation

IoT devices must meet ANATEL's cybersecurity and equipment certification rules, outlined in Resolution No 715/2019, Resolution No 740/2020, and Act No 77/2021. These regulations include "Security by Design" requirements to ensure devices are secure by default and resilient to cyber threats.

Industry Codes of Conduct

ABINC and ABNT Standards

In late 2025, the Brazilian Association of Internet of Things (ABINC) and the Brazilian Association of Technical Standards (ABNT) published new technical standards focused on IoT interoperability and cybersecurity. These standards are designed to improve device compatibility, strengthen security practices, and support the development of a safer and more integrated IoT ecosystem.

4.2 Compliance and Governance

Compliance Challenges for IoT Deployment

Permanent roaming

A common challenge for IoT deployments – such as connected vehicles or logistics trackers – is Brazil's restriction on permanent roaming. ANATEL prohibits foreign SIM cards from using Brazilian networks for more than 90 consecutive days. If an IoT fleet depends on global SIMs that do not switch to a local profile, Brazilian operators are legally permitted to block those devices once the limit is exceeded.

Hardware homologation and cybersecurity

All telecommunications devices and equipment must undergo ANATEL certification and homologation before they can be used in Brazil. Cybersecurity requirements for these devices are outlined in ANATEL Act No 77/2021, which establishes obligations such as Security by Design and other measures intended to ensure robustness and resilience.

Data protection

IoT deployments typically involve large-scale processing of personal data – from smart-home systems and wearables to urban monitoring devices. As a result, they fall under the scope of Brazil's General Data Protection Law (LGPD) and are subject to oversight by the ANPD.

Regulatory fees

M2M devices may qualify for exemptions from certain telecommunications fees under Law No 14,108, provided they meet the legal criteria for M2M classification.

Governance Frameworks

To address these compliance risks effectively, companies should adopt an integrated governance framework that includes the following.

- Technical standards – implement ABNT standards and industry best practices alongside all applicable regulatory requirements.
- Privacy management – apply LGPD principles through Privacy by Design, supported by continuous monitoring and periodic compliance audits.
- Legal oversight – manage cross-cutting legal obligations, including those related to consumer protection, intellectual property, and contractual arrangements.

4.3 Data Sharing

Key Legal Requirements for IoT Data Sharing

All handling of personal data – including its collection, processing, storage, transfer, and deletion – is governed by the General Data Protection Law (LGPD). When sharing personal data with third parties, companies must:

- Obtain valid consent from data subjects for any third-party sharing.
- Clearly inform data subjects about how their data will be used and the purposes of sharing.
- Rely on an appropriate LGPD legal basis for processing, such as consent, contractual necessity, or legitimate interest.
- Implement technical and administrative safeguards to prevent unauthorised access, misuse, or data breaches.

Applicability

The LGPD applies to any organisation that processes personal data when:

- the processing activity takes place in Brazil;
- the organisation offers goods or services to individuals located in Brazil or processes their data; or

• the personal data was originally collected in Brazil.

There are no minimum thresholds for applicability. Organisations that process large volumes of data or handle sensitive categories (such as health, biometric, or children's data) must comply with stricter requirements.

Sensitive Data

The LGPD imposes enhanced protections for sensitive personal data, which includes information about racial or ethnic origin, religious beliefs, political opinions, union membership, health or sex life, and genetic or biometric data. Processing this type of data requires a specific legal basis, such as explicit consent, compliance with legal obligations, health protection, or safeguarding the life and safety of individuals.

Additional protective measures, including stricter access controls and strengthened security practices.

5. Audiovisual Media Services

5.1 Requirements and Authorisation Procedures

Broadcasting (TV and Radio)

Broadcasting in Brazil is heavily regulated under the Federal Constitution, the Brazilian Telecommunications Code (Law No 4,117/1962), and Decree No 52,795/1963.

Key requirements

Free-to-Air (FTA) TV and radio

FTA broadcasting is considered a public service provided by private companies through concessions, permissions, or authorisations granted by the Executive Branch and approved by Congress.

Programming obligations

Broadcasters must:

• prioritise educational, cultural, artistic, and informational programming;
• promote national and regional culture, as well as independent production;
• comply with regional content quotas; and
• respect ethical and social values of individuals and families.

Ownership rules

Ownership and editorial control of broadcasting and journalism companies are restricted to:

• Brazilian-born citizens;
• naturalised citizens with at least ten years of nationality; or
• legal entities incorporated in Brazil with headquarters in the country.

At least 70% of voting capital must be held by these qualifying individuals, who must also be responsible for management, editorial decisions, and programming content. These responsibilities cannot be delegated to non-eligible individuals.

Procedures and fees

• Public bidding – licences are awarded via public tenders requiring qualification documents and technical and price proposals.
• Granting act – issued by the Communications Minister (for radio) or the President (for FTA TV), followed by congressional approval.
• Licensing – after approval, companies have 12–18 months to obtain frequency authorisation and operating licences from ANATEL and must pay applicable frequency-use fees and FISTEL taxes
• Contract and payment – the concession contract is finalised after submission of required documents and payment of the concession fee.

Regulation of Pay-TV

Pay-TV services fall under the telecommunications regulatory framework, primarily Law No 12,485/2011 and ANATEL regulations.

Key requirements

Must-carry obligations

Pay-TV providers must include certain mandatory channels in all packages, including:

• local FTA broadcasters;
• legislative, judicial, and executive branch channels;
• educational, cultural, community, and citizenship channels; and

- municipal/state legislative and university channels.

Cross-ownership restrictions

- Telecommunications providers cannot have more than 50% of their equity and voting capital controlled by broadcasting concessionaires, licensees, content producers, or programmers.
- Broadcasting companies cannot have more than 30% of their equity and voting capital controlled by telecom operators.
- Each type of entity is prohibited from directly offering the other's services.

Procedure and fees

- Authorisation – companies must obtain ANATEL authorisation to provide collective-interest telecommunications services and must notify ANATEL of the Pay-TV offering.
- Fee – telecom service authorisation requires a fee of BRL400.00.

Digital Media: Streaming and Video-Sharing Platforms

Video-on-Demand (VoD) services operate under a free-enterprise regime and are not currently subject to the same obligations as broadcasting or Pay-TV companies.

However, pending legislation – such as Bill No 8,889/2017 and Bill No 2,331/2022 – proposes imposing Brazilian content quotas and requiring payment of CONDECINE contributions.

6. Telecommunications

6.1 Scope of Regulation and Pre-Marketing Requirements

Technologies and Services Covered by Telecom Regulations

Regulated services

- mobile telephony (4G/5G);
- fixed broadband (fibre-based internet service providers);
- fixed telephony (traditional landline services); and
- pay-TV services (cable and satellite).

Non-regulated services

- Value-Added Services (VAS) such as OTT platforms and cloud services.

Hybrid or Conditional Cases

Data centres

Data centres must obtain ANATEL certification when they operate integrated with telecommunications networks, in accordance with Resolution 780/2025.

Marketplaces

Marketplaces are not considered telecom service providers, but they can be held jointly liable when advertising or selling non-certified telecommunications equipment, also under Resolution 780/2025.

Equipment Certification Requirements

All telecommunications equipment must be certified and homologated by ANATEL.

Certification requirements include the cybersecurity obligations set out in Act No 77/2021, which mandate:

- security by design;
- privacy by design; and
- maintenance of updated security and privacy policies.

Security Requirements

Cybersecurity

Telecom operators must audit their suppliers of software, equipment, and components to ensure compliance with ANATEL's cybersecurity standards.

Data centres integrated into telecom infrastructure must comply with physical security and cybersecurity resilience rules.

Secrecy of communications

Brazilian law guarantees the confidentiality and inviolability of communications.

Interception is only allowed under a court order for criminal investigations, pursuant to Law No 9,296/1996.

These protections apply to telephone, computer, and telematic systems.

6.2 Net Neutrality Regulations

Legal Framework

Internet Law (Law No 12,965/2014, Article 9)

Internet service providers and telecommunications operators must treat all data packets equally, regardless of their content, origin, destination, service, device, or application.

Regulatory Decree (Decree No 8,771/2016)

The decree reinforces that traffic discrimination for commercial purposes is strictly prohibited. For example, a telecom operator cannot slow down a competing streaming service to promote its own, nor can it sell paid "fast lanes."

Exceptions:

- Technical requirements such as spam filtering, DoS mitigation, or congestion management, provided the measures are proportional, transparent, and non-discriminatory.
- Prioritisation of emergency services is permitted.

Sector Impact

Zero-rating

Zero-rating offers – such as mobile plans that provide "free social media" usage – remain largely allowed. Regulators generally interpret the law as prohibiting throttling but not exempting specific apps from data caps, so long as competition is not harmed.

5G and network slicing

5G network slicing, which creates virtual network segments with guaranteed speed or latency for specific applications (such as hospital robots or autonomous vehicles), is treated as a technical capability rather than a violation of net neutrality. This is because it does not degrade other traffic.

Network fee debate

Mirroring discussions in Europe, Brazilian telecom operators advocate for a "network fee" that would require major content providers to contribute to infrastructure costs. Large global platforms oppose the proposal, arguing that it undermines net neutrality by differentiating between traffic sources. The debate remains ongoing and unresolved.

6.3 Emerging Technologies

Impact of Emerging Technologies on the Legal Landscape

Regulatory expansion and new incentives

The rapid growth of 5G, IoT, AI, and related technologies has prompted significant updates across Brazil's regulatory environment. ANATEL is transitioning from its traditional, telecom-centric focus toward broader oversight of digital platforms and infrastructure. Its priorities now include equipment approval, cybersecurity, critical-infrastructure resilience, sustainability requirements, and energy-efficiency standards.

Other agencies are also expanding their authority. Law No 14,815/2024 strengthened ANCINE's powers – allowing it to suspend or terminate the unauthorised use of both Brazilian and foreign audiovisual works. ANCINE's current agenda emphasises restructuring the audiovisual sector and responding to the rapid rise of VoD platforms.

Under Decree No 12,622/2025, the ANPD gained new responsibilities related to protecting children and adolescents online, giving it the authority to enforce the Youth Law and issue implementing regulations.

Brazil is also moving forward with Bill No 4,675/2025, the "Fair Competition Act for Digital Markets." This proposal seeks to introduce ex ante rules for digital platforms. It grants CADE powers to identify potential gatekeepers and impose tailored obligations on them.

Fragmented digital governance

Despite these developments, Brazil's digital governance framework remains fragmented. Multiple entities – including Congress and agencies such as ANATEL, CADE, ANCINE, and ANPD – continue to share overlapping responsibilities, creating a complex regulatory landscape.

Artificial intelligence

AI technologies are increasingly integrated into telecom operations, supporting functions such as network optimisation, predictive maintenance, and customer service automation. ANATEL itself is using AI to modernise regulatory oversight and enhance operational efficiency.

To avoid hindering innovation, ANATEL has so far adopted a principle-based approach to AI regulation. However, updates to its Regulatory Oversight Regulation are expected and may introduce new obligations for regulated entities, including:

- allowing ANATEL access to AI-based equipment, systems, applications, and tools they use;
- providing ANATEL with data used to train AI models and other supporting technical documentation; and
- permitting ANATEL to employ automated processes, including AI, for monitoring and enforcement.

At the national level, Brazil is progressing on an AI Act (Bill 2,338/2023), aligned with the EU's risk-based model and establishing obligations based on system risk categories.

Key Legal Considerations for Companies

Data sovereignty and privacy

Companies must ensure that the collection, processing, storage, and international transfer of personal data comply with the LGPD and relevant rules on data localisation and cross-border data flows.

Cybersecurity audits

Telecom providers and their suppliers must undergo mandatory cybersecurity audits. Hardware must also comply with security-by-design and privacy-by-design principles.

Telecom licensing

Businesses should assess whether their operations constitute regulated telecommunications services and determine which ANATEL license – if any – is required for lawful operation.

Equipment certification

Before launching, importing, or selling equipment in Brazil, companies must verify whether their devices fall under ANATEL's certification and homologation requirements and plan for testing and approval timelines.

Monitoring a Rapidly Evolving Landscape

Given the pace of technological and regulatory change, companies operating in Brazil should closely monitor legislative developments, regulatory guidance, and enforcement trends. Proactively adjusting compliance programmes will be critical to meeting new obligations and mitigating regulatory risk.

7. Challenges With Technology Agreements

7.1 Legal Framework Challenges

Main Challenges in Entering Technology Agreements in Brazil

Regulatory complexity and fragmentation

Brazil's legal landscape blends general civil law principles with numerous sector-specific rules, such as the LGPD, the Internet Law, and ANATEL regulations. This creates practical challenges when drafting agreements for emerging technologies – including AI, cloud, and IoT – because obligations may derive from multiple overlapping regulatory regimes.

Data protection compliance (LGPD)

The LGPD imposes strict requirements on the processing, sharing, and international transfer of personal data. Technology contracts must clearly define the parties' roles and responsibilities, establish appropriate legal bases for processing, and include safeguards for cross-border data transfers.

Infrastructure and service classification issues

When dealing with cloud services, data centre arrangements, software, or connectivity, it is often difficult to determine whether ANATEL's telecommunications rules apply – particularly where the services blur the line between IT and telecom activities.

Cybersecurity obligations

Multiple sectors impose mandatory cybersecurity requirements, including incident reporting, technical standards, and audit rights (eg, under ANATEL regulations). As a result, technology agreements frequently require detailed language to address these obligations.

Key Features of the Brazilian Legal Framework to Consider

Currency and price adjustment

Domestic contracts must be priced and paid in Brazilian reais (BRL), pursuant to Article 1 of Law No 10,192/2001 and Article 318 of the Civil Code (Law No 10,406/2002). International contracts involving at least one foreign party may use foreign currency under Article 13 (II) of Law No 14,286/2021.

Brazil also recognises the principle of economic–financial balance in long-term contracts, meaning certain circumstances may justify price revisions under the Civil Code, the Consumer Protection Code, or public procurement rules (where a government entity is a contracting party).

Governing law and dispute resolution

Under Article 9 of the LINDB, the law applicable to a contract is generally the law of the place where the obligation is constituted. If an agreement is formed in Brazil – or if the offeror is based in Brazil – Brazilian law will typically govern. Even where a foreign forum is selected, Brazilian courts may assert jurisdiction when obligations are performed in Brazil. Foreign law may validly govern the contract when arbitration is chosen.

Data storage and privacy (LGPD)

Brazil does not require data localisation. However, the LGPD imposes stringent rules on international transfers, including adequacy requirements, contractual guarantees, and other mechanisms to ensure protection levels consistent with Brazilian standards.

Consumer protection considerations

Certain contractual clauses – such as broad liability waivers or unilateral modification rights – may be considered abusive and unenforceable if one of the contracting parties qualifies as a consumer.

Telecommunications regulations

If the agreement touches on telecommunications or connectivity services, ANATEL may impose mandatory obligations, such as equipment certification, licensing, and cybersecurity standards.

Public procurement rules (if applicable)

Technology contracts involving public entities must comply with Law No 14,133/2021, which includes mandatory provisions relating to risk allocation, audit rights, transparency, and performance monitoring.

Intellectual property and software licensing

Brazilian software legislation (Law No 9,609/1998) affects licensing structures, liability allocation, and in some cases the registration of software-related agreements for tax or commercial purposes.

Tax considerations

Brazil's tax system is highly complex, and technology agreements must be drafted with attention to tax implications – including potential exposure to indirect taxes, withholding, and service classifications – to avoid unintended liabilities.

7.2 Service Agreements and Interconnection Agreements

Key Elements in Telecom Agreements

Service Level Agreements (SLAs)

In Brazil, SLAs are not only commercial best practices but often align with regulatory quality indicators. Contracts should clearly define metrics such as Mean Time to Repair (MTTR) and response times. ANATEL regulations also require automatic discounts for service interruptions, meaning agreements must include strong liability and indemnity provisions.

Regulatory compliance

Telecom agreements must ensure strict compliance with the General Telecommunications Law (LGT), ANATEL's regulatory framework, and applicable consumer protection rules.

Data protection

Contracts must include provisions compliant with the LGPD, addressing:

- technical and security measures;
- incident and breach-notification obligations; and
- allocation of responsibilities for data-processing activities.

Network operations and maintenance
Operational responsibilities must be clearly allocated, including:

- maintenance windows and planned outages;
- notice periods;
- fault-reporting processes; and
- facility access and field operations.

Dispute resolution
Effective mechanisms for resolving technical and commercial disputes should be established. Common tools include escalation paths, dispute boards, and arbitration clauses.

Secrecy of communications
Agreements must ensure the confidentiality of all communications transmitted through the network, in line with Brazilian laws on the inviolability of communications.

Liability and indemnities
Contracts should establish a balanced allocation of risk, addressing:

- liability caps and carve-outs (eg, gross negligence, data breaches, wilful misconduct);
- indemnification for regulatory penalties caused by the counterparty; and
- allocation of responsibility for service credits imposed by regulation.

Unbalanced clauses may be deemed void by the Brazilian Judiciary, which is known to intervene in private agreements.

Favourable Terms for Negotiation
- Volume and duration – higher volumes or longer commitments may justify discounts, enhanced SLAs, or waivers on exclusivity.
- Exclusivity – when appropriate, exclusivity may be leveraged to obtain better pricing and service conditions.
- Audit rights – billing audit clauses can allow withholding of disputed amounts.
- Risk allocation – liability caps should be proportionate, indemnities reciprocal, and force majeure clauses adapted to telecom realities (eg, fibre cuts, tower damage, and power failures).

Interconnection Agreements (Wholesale)
Regulatory framework
Interconnection arrangements are governed by the General Regulation of Interconnection (RGI – ANATEL Resolution No 693/2018).

Key considerations
Public offer (OPI)
Common carriers must publish an ANATEL-approved OPI, which serves as a reference – often a ceiling – for pricing and conditions during negotiations.

Mandatory clauses
Interconnection agreements must include financial-settlement mechanisms, fraud-prevention measures, and well-defined operational processes.

Anti-competitive conduct
The RGI prohibits practices such as withholding technical information, discriminatory treatment, or imposing unreasonable contractual conditions.

Artificial traffic
Contracts must contain anti-fraud provisions to detect and prevent robotic calling patterns, inflated traffic, or other manipulations.

Resource sharing
Parties may share equipment, infrastructure, and facilities to support interconnection. Agreements should specify technical standards, pricing structures, and operational responsibilities for such sharing.

8. Trust Services and Digital Entities

8.1 Trust Services and Electronic Signatures/ Digital Identity Schemes
Laws and Regulations: Trust Services and Electronic Signatures
MP 2.200-2/2001 remains the foundation of Brazil's digital trust framework, establishing ICP-Brasil, the Brazilian Public Key Infrastructure.

Qualified electronic signatures (certificado digital)
Signatures supported by an ICP-Brasil certificate carry a legal presumption of authenticity and validity.

Private electronic signatures
Article 10, Section 2 confirms that other forms of electronic signatures are valid as long as the parties agree to their use and the document's integrity is not disputed.

Law No 14.063/2020 introduced a tiered structure for electronic signatures used in interactions with the public sector.

- Simple electronic signature – identifies the signatory and links the signature to specific electronic data.
- Advanced electronic signature – ensures authorship and integrity, is uniquely associated with and controlled by the signatory, and allows detection of any later modification.
- Qualified electronic signature – requires certification under the ICP-Brasil infrastructure.

The ICP-Brasil Technical Standards (DOC-ICP) define the technical, operational, and security requirements for issuing and managing ICP-Brasil certificates. Compliance is mandatory for Certification Authorities (CAs), Registration Authorities (RAs), and all entities participating in the trust chain.

Elements for Consideration

Cross-border recognition (Mercosur Agreement)
Under Decree No 12.376/2025, Brazil now recognises digital signatures issued in Argentina, Paraguay, and Uruguay – and these countries reciprocate. This change enhances the execution of regional commercial and governmental agreements.

Data protection (LGPD)
Digital identity systems often use biometric data (such as facial images or fingerprints), which are classified as Sensitive Personal Data under the LGPD. Processing this data requires:

- a valid legal basis;
- strong security and governance measures; and
- appropriate incident and breach notification procedures

9. Gaming Industry

9.1 Regulations

Brazil's gaming industry is now regulated under a modernised framework that clearly distinguishes electronic games from gambling ("bets"), with each category subject to its own compliance obligations.

Core Laws and Regulations

Legal Framework for Games (Law No 14,852/2024)
This law establishes Brazil's first comprehensive regulatory framework for electronic games. Its key provisions include:

- a formal definition of electronic games;
- special customs regimes that reduce import costs for development kits, VR equipment, and similar technologies, along with cultural-sector incentives;
- measures to protect children and adolescents; and
- a national age-rating system.

Bets Law (Law No 14,790/2023)
This law regulates sports betting and online gambling, drawing a clear boundary between gambling and electronic games. Any game that offers monetary prizes based on random outcomes is classified as a "bet".

Its main provisions include:

- mandatory licensing requirements;
- ownership and financial standards for operators;
- advertising rules;
- anti–money laundering and counter-terrorism financing obligations; and
- administrative penalties, including fines and potential suspension.

The Secretariat of Prizes and Betting (*Secretaria de Prêmios e Apostas* – SPA) within the Ministry of Finance oversees the gambling sector. SPA's regulations cover licensing procedures, technical standards, monitoring, sanctions, and general oversight.

Industry Self-Regulation

CONAR

As noted earlier, CONAR sets widely respected advertising standards that apply to gaming and betting platforms. Although adherence is voluntary, compliance is effectively mandatory in practice because media outlets routinely remove non-compliant advertisements. CONAR also maintains specific standards for gambling-related advertising.

Key legal challenges

Brazil's gaming sector faces increasing scrutiny regarding protections for minors, age restrictions, loot boxes, randomised rewards, and monetisation systems that resemble gambling. Recent laws have introduced new limitations on minors' access to such features.

Law No 14,790/2023 already prohibits betting activities for minors, and CONAR requires 18+ warnings and bans advertising directed at children. In addition, Ordinance No 1,048/2025, approved by the Ministry of Justice and Public Security (MJSP), strengthens these protections. Companies must comply fully by 17 March 2026.

The industry must also adapt to Brazil's broader tax reform and the introduction of the split-payment regime, as referenced in **1.3 Digital Economy Taxation**.

9.2 Regulatory Bodies

Primary Regulatory Bodies

Regulation of Brazil's gaming industry is divided among several governmental authorities, each operating within its legally defined mandate. The Ministry of Finance, through the SPA, functions as the central regulator for licensed gambling and betting activities. The MJSP oversees age-rating classifications for digital games and audiovisual content through the ClassInd system. In addition, the National Data Protection Authority (ANPD) may exercise jurisdiction over gaming operators whenever their activities involve the collection or processing of personal data.

Recent Enforcement Actions

Between late 2024 and 2025, Brazil undertook its most significant enforcement measures to date in the online gaming and betting sector. After the licensing grace period expired, the SPA released a comprehensive "Negative List" identifying more than 2,000 unlicensed gambling platforms. This list was submitted to ANATEL, triggering a nationwide operation requiring Internet service providers to block access to the domains of these non-compliant platforms. As a result, several major international brands that had not begun the licensing process became inaccessible to users in Brazil.

This enforcement effort created a clear division within the market: a regulated "white market" composed of licensed operators authorised to use the. bet.br domain, and an unregulated "black market" made up of platforms facing access restrictions due to non-compliance.

9.3 Intellectual Property

Common IP Challenges Faced by Game Developers in Brazil

Multiplicity of IP regimes and layered rights

A single video game usually incorporates several types of intellectual property: software (source code), audiovisual content (graphics, music, narrative), character and brand identity, and sometimes functional or technical innovations. Developers must choose which IP regimes are most appropriate – software copyright, general copyright, trade marks, industrial design, or patents.

Overlapping protection and registration uncertainty

Software is protected both under the Computer Programs Act (Law 9.609/98) and the general Copyright Law (Law 9.610/98). Other components – such as music, art, or audiovisual elements – are covered by copyright as well. Because certain elements (especially visual or design components) can potentially fall under multiple regimes, developers often face uncertainty about how to structure their registrations and safeguard each asset.

Enforcement challenges, especially with piracy

As in many countries, Brazilian developers struggle with unauthorised copying, distribution, and "modding," including dissemination over the internet.

Enforcing rights can be difficult and resource-intensive.

Recent legal developments and resulting uncertainty

The new "Videogame Act" (Law 14.852/2024) introduces opportunities but also new questions. It creates a specific registration category for electronic games at the National Institute of Industrial Property (INPI), which may require companies to update internal compliance and administrative processes.

Rights of Creators to Protect IP in Virtual Environments

Creators are protected under both the Software Law (Law 9.609/98) and the Copyright Law (Law 9.610/98). Source code is treated as a literary work, while graphics, story elements, music, and design are protected as artistic or audiovisual works.

Law 14.852/2024 formally recognises games – including console, mobile, web, VR/AR/MR/XR formats – as interactive audiovisual works or software, strengthening their eligibility for multiple types of IP protection.

For industrial property concerns, developers may also rely on trademarks, industrial design registrations, or patents if the game involves technical innovations. Registration with INPI or other competent authorities – particularly under the new videogame-specific registration scheme – can strengthen enforcement and evidentiary rights in licensing or litigation.

Key Considerations for Copyright in Digital and Virtual Assets

Automatic protection

Copyright protection exists from the moment a work is fixed, regardless of registration. Registration is optional but useful for proving authorship.

Duration of protection

Software is protected for 50 years (starting 1 January of the year following creation or publication) under Law 9.609/98. Other works – such as art and music – follow the standard term under Law 9.610/98.

Clear separation of elements:

To maximise protection, developers should document and separate code, audiovisual assets, narrative, character design, and other components. Consolidating rights through contracts is essential, especially when multiple contributors are involved. When possible, developers should register works at INPI or other relevant authorities.

Digital piracy risks

Given the ease of online copying, streaming, and distribution – including user-created modifications – developers must use technical protection measures and be prepared to pursue civil or, when applicable, criminal action.

Application of Industrial Property Law to Virtual Goods and Services

Under the Industrial Property Law (Law 9.279/96), any visually perceptible distinctive sign may be registered as a trademark with INPI. This includes game titles, logos, franchise names, character names, and potentially in-game brands.

Traditional principles still apply:

- Speciality – protection covers only the registered classes of goods/services.
- Territoriality – protection applies only within Brazil.

In global virtual environments – such as online multiplayer worlds or games hosted on international servers – these principles can create uncertainty. Developers seeking broader protection should consider trade mark registration in additional jurisdictions or use agreements and licences that address cross-border virtual distribution.

Implications of User-Generated Content (UGC) for IP Rights

User-generated content (mods, custom assets, skins, levels, stories, etc.) can create complex IP issues. The base game is protected by copyright and possibly by trade marks, so derivative works may infringe unless they fall under a valid licence.

Developers should:

- Use clear EULAs, Terms of Service, and licensing agreements that specify what rights users have when creating UGC.
- Define whether commercial use is allowed, whether rights are licensed back to the developer, and how revenue (if any) is handled.

Because copyright arises automatically under Brazilian law, unauthorised derivative works or distribution may be actionable, though enforcement can be difficult in cross-border or virtual environments.

The new videogame legislation strengthens the legal basis for asserting exclusive rights over derivative uses but does not replace the need for careful licensing and rights management.

Key Takeaways and Strategic Recommendations for Developers in Brazil

- Use multiple IP tools together – protect software and audiovisual works under copyright, register trade marks for titles and brands, and consider design or patent protection when applicable.
- Leverage INPI registration – including the new videogame-specific category – to reinforce enforceability.
- Draft clear contracts with collaborators, artists, musicians, and other contributors to consolidate rights.
- Implement strong EULAs and licensing terms for end users, especially concerning mods and UGC.
- Actively monitor unauthorised distribution and pursue enforcement through civil or, where appropriate, criminal measures.

10. Social Media

10.1 Laws and Regulations for Social Media

Laws and Regulations Relevant to Social Media in Brazil

Brazil does not yet have a single, comprehensive law regulating all social media platforms operating in the country. Instead, several key legal frameworks currently apply.

Brazil's Internet Law (Law No 12,965/2014)

This law establishes rights, guarantees, and duties related to internet use, including rules for application providers.

Important update

In June 2025, the Brazilian Supreme Court (STF) ruled that platforms may be held civilly liable – even without a court order – if they fail to remove content that is manifestly illegal (such as terrorism, racism, or violence against women and children) or where systemic moderation failures occur.

Until new legislation is introduced, platforms must:

- remove unlawful content and fake accounts following takedown requests; and
- implement self-regulation measures such as clear notification systems, due process mechanisms, transparency reporting, and accessible support channels.

Youth Law (Law No 15.211/2025)

This law establishes broad protections for children and adolescents in digital environments. It applies to any digital product or service directed at – or likely to be accessed by – minors, including social media platforms.

Key obligations for providers include the following.

- Setting default privacy protections and preventing misuse of minors' personal data.
- Avoiding features that encourage compulsive use.
- Moderating harmful content such as sexual exploitation, violence, cyberbullying, self-harm, gambling, and misleading advertising.
- Removing and reporting illegal material and ensuring age-appropriate content.
- Implementing effective age verification, obtaining parental consent for app downloads, providing clear risk information, and ensuring accessible parental controls.
- Prohibiting profiling for targeted advertising and the monetisation of sexualised content involving minors.

Effective date: enacted in September 2025; enforcement begins in March 2026.

Key Legal Challenges Related to Social Media Regulation

Brazil faces several ongoing challenges in regulating social media platforms, including the following.

- Legal uncertainty regarding the new liability standards imposed by STF rulings (Themes 987 and 533).
- Balancing fundamental rights – such as freedom of expression – with the need for regulation.
- Addressing economic and competitive issues, as major platforms operate across multiple sectors where traditional regulatory models may not apply.
- Establishing effective governance and enforcement structures, given the lack of a specialised regulatory body for digital services and competing claims among different government agencies.

10.2 Regulatory and Compliance Issues

Regulatory Landscape for Social Media Oversight in Brazil

Brazil does not have a single, dedicated regulator for social media platforms. Instead, oversight has largely been driven by the Judiciary, which has taken an increasingly active role in ordering content removals and, in some cases, imposing service suspensions when platforms fail to comply with judicial decisions.

Judicial enforcement

An important example occurred in August 2024, when the Brazilian Supreme Court (STF) ordered a nationwide blocking of X (formerly Twitter) after repeated noncompliance with court orders. The platform was restored only after paying significant fines, appointing a legal representative in Brazil, and fulfilling directives to deactivate specific accounts.

Agencies Signalling Regulatory Intent

National Data Protection Authority (ANPD)

Since 2025, the ANPD has taken on a central role in enforcing the Youth Law (Law No 15,211/2025), which sets rules for products and services directed at minors – including social media.

The Agency has been designated as the autonomous authority responsible for safeguarding children and adolescents online.

Its responsibilities include monitoring compliance, issuing regulations, and ensuring enforcement.

Administrative Council for Economic Defense (CADE)

CADE has intensified scrutiny of digital markets since 2022, conducting investigations into anticompetitive conduct and applying precautionary measures.

In 2025, Bill No 4,675/2025 was introduced, creating an ex ante regulatory framework for digital platforms and expanding CADE's authority in the sector.

National Telecommunications Agency (ANATEL)

Since 2021, ANATEL has broadened its regulatory focus to include digital platforms and infrastructure intermediaries.

Current initiatives aim to treat digital platforms as users of telecom networks, enabling the Agency to apply measures that promote network sustainability.

11. Data Privacy and Cybersecurity

11.1 Data Privacy in Telecommunications

Key Data Privacy Laws and Regulations for Telecom Providers in Brazil

Primary legal framework

Brazil's privacy landscape is grounded in several key instruments.

- Federal Constitution – ensures the fundamental right to privacy and protection of personal data.
- General Data Protection Law (LGPD – Law No 13,709/2018) – the primary data protection law applicable across all sectors, supplemented by regulations issued by the National Data Protection Authority (ANPD).
- *Marco Civil da Internet* (Law No 12,965/2014) – governs data collection, storage, and processing by internet and connectivity providers.

While the ANPD is the central authority overseeing privacy and data protection, ANATEL also imposes sector-specific obligations through instruments such as its Cybersecurity Regulation and General Telecommunications Services Regulation, which require privacy-by-design measures and mandate prior consent for sharing subscriber data.

Key Challenges in Managing Customer Data Privacy

Telecom operators face several privacy-related challenges.

High volume and sensitivity of data

Providers handle vast amounts of personal information – such as subscriber details, call metadata, geolocation, and browsing data – significantly raising compliance complexity and security risks.

Strict LGPD requirements

The LGPD mandates explicit consent, clear internal policies, mechanisms for data subject rights, and strong technical and organisational security controls. Achieving full compliance often requires substantial investment.

Third-party and vendor management

Operators rely heavily on outsourced services (eg, cloud hosting, network management). Ensuring these partners maintain adequate privacy and security standards is critical.

Cybersecurity risks

Increased cyber threats require robust protective measures, including encryption, network segmentation, intrusion monitoring, and advanced firewalls.

Cross-Border Data Transfers and Data Localisation

International transfers of personal data are regulated under the LGPD and ANPD Resolution No 19/2024. Transfers are allowed only when appropriate safeguards exist, such as the following.

- Adequacy decisions – when ANPD recognises that another jurisdiction provides equivalent data protection.
- Standard contractual clauses (SCCs) – ANPD-approved clauses ensuring LGPD-level protection abroad.
- Equivalent standard clauses – clauses approved by foreign authorities or international bodies that ANPD deems comparable to Brazilian SCCs.
- Specific contractual clauses – used in exceptional situations where SCCs are not suitable.
- Binding Corporate Rules (BCRs) – internal rules for multinational groups, requiring ANPD approval, to govern transfers within the same corporate group.

Balancing Lawful Interception and Privacy

Brazil's Constitution protects the confidentiality of communications, allowing interception only through a court order for criminal investigations as defined under Law No 9,296/1996.

Telecom operators must comply while still safeguarding privacy. Common practices include the following.

- Data segregation – ensuring only the court-mandated data is disclosed.
- Strict internal protocols and audits – tracking and controlling access to intercepted information.
- Advanced security measures – encryption and protections to shield data unrelated to the investigation.
- Governance and legal oversight – legal teams validate and monitor compliance with lawful-interception requests to prevent misuse.

Role of Third-Party Vendors and Cloud Providers

Telecom providers increasingly rely on external vendors and cloud services for infrastructure and data processing. ANATEL's Cybersecurity Regulation requires suppliers to adopt privacy-by-design practices and to undergo independent audits, ensuring the security of the broader telecom ecosystem.

Impact of Evolving Data Privacy Regulations on Infrastructure and Innovation

Emerging regulatory demands significantly influence network design and technological innovation.

Strengthened infrastructure requirements
Operators must invest in resilient, secure networks with strong encryption, continuous monitoring, and controlled access to satisfy LGPD obligations.

Privacy-by-design integration
Privacy considerations must be embedded into network architecture, product development, and operational processes from the outset.

Effects on emerging technologies
Technologies such as IoT, AI, cloud computing, and big data depend on massive data flows. Privacy rules introduce additional layers of consent management, security, and governance, increasing operational complexity and costs.

Cross-border data transfer challenges
Telecom networks routinely process international traffic. Limited adequacy decisions and ANPD's evolving enforcement capacity create uncertainty for operators managing global data flows.

11.2 Cybersecurity in Digital Media and Streaming Services

Legal and Operational Challenges in Data Privacy for Digital Media and Streaming Services

Balancing innovation and privacy
Digital media and streaming providers face a central challenge: how to innovate while managing the risks associated with intensive data use. Because regulation often develops more slowly than technology, companies must simultaneously ensure:

- full compliance with Brazilian data protection regulations; and
- a genuine ethical commitment to privacy and responsible data handling.

Achieving this balance requires a multidimensional approach that strengthens internal governance and builds external trust.

Internal Measures

Companies need to promote a culture rooted in ethics and data protection, supported by strong governance structures. Essential practices include:

Privacy-by-design and security-by-design
Integrating privacy safeguards from the earliest stages of product development, making privacy the default setting, and incorporating techniques such as encryption, anonymisation, and secure coding.

Data Protection Impact Assessments (DPIAs)
Conducting assessments for activities that present high risks to data subjects.

Transparency and user control
Ensuring users clearly understand how their data is collected, used, stored, and managed.

External Measures

Building and maintaining user trust is fundamental. Digital service providers should:

- communicate consistently and transparently about data practices;
- reduce reputational and regulatory risks through openness; and
- present privacy as a competitive differentiator in a market increasingly focused on digital ethics.

Challenges in Third-Party Data Sharing

When sharing data with advertisers, analytics companies, or business partners, providers must comply with the LGPD, which requires:

- valid consent for any third-party data sharing; and
- clear disclosure of the purpose and scope of such sharing.

Additionally, the Youth Law (Law No 15,211/2025) prohibits the use of profiling techniques for targeted advertising directed at minors, adding further restrictions for platforms that serve young audiences.

Impact of Emerging Cybersecurity Regulations

Brazil does not yet have a dedicated cybersecurity law specifically for digital media platforms. However, national initiatives – such as the National Cybersecurity Strategy and National Cybersecurity Policy – establish guidelines applicable to all sectors. These include:

- implementing cybersecurity and risk management measures; and
- developing mechanisms to prevent, mitigate, and respond to vulnerabilities and cyber-attacks.

Future regulatory developments aligned with these initiatives may impose new obligations, such as:

- minimum security standards;
- structured risk-mitigation processes; and
- increased operational costs for digital platforms and operators of critical infrastructure.

Trends and Developments

Contributed by:
Tomás Paiva, Vitor Amorim, Caio Moura and Rebeca Cabral
Pinheiro Neto Advogados

Pinheiro Neto Advogados has rendered legal services in all legal areas since 1942 and has the structure to offer its clients comprehensive assistance with their business activities. The firm provides services to approximately 2,000 local and international groups, and has offices in São Paulo, Rio de Janeiro, Brasília, Palo Alto and Tokyo. With over eight decades of experience and clients spanning more than 80 countries, the firm has developed a unique, tight-knit culture focused on ever-improving the delivery of legal services in Brazil. Pinheiro Neto Advogados has lawyers specialising in all areas of law.

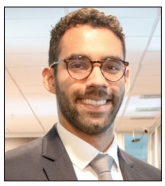
Authors



Tomás Paiva advises Brazilian and international clients on regulatory and contractual matters in the technology, media and telecommunications (TMT) and infrastructure sectors. His practice encompasses regulatory advisory work – including regular engagement with key regulatory authorities such as ANATEL and ANCINE – as well as the structuring and negotiation of complex transactions involving TMT-related products and services. Tomás has extensive experience across a broad range of technologies and regulatory frameworks, having advised on major transactions in the sector, and has built a strong track record in securing regulatory approvals.



Vitor Amorim advises Brazilian and international clients on regulatory, contractual, and transactional matters related to infrastructure and public law, with a particular focus on the technology, media and telecommunications (TMT) sector. He has broad experience across all verticals of the TMT industry, including mobile services, fibre optics, satellites, passive infrastructure, and OTT platforms. Amorim brings a strong transactional focus to his practice, regularly assisting clients in the design and structuring of business models within the sector. He also has an established track record in administrative and judicial litigation and has advised TMT clients on landmark legal disputes.



Caio Moura advises domestic and international clients on litigation, contracts, and regulatory and transactional matters in public law across the technology, media and telecommunications (TMT) and infrastructure sectors. His expertise includes complex and innovative matters involving telecommunications services, radio spectrum use, infrastructure sharing, critical infrastructures, internet applications, new technologies regulation, and the structuring and regulatory approval of complex businesses and transactions.



Rebeca Cabral advises domestic and international clients on regulatory and transactional matters in the technology, media and telecommunications (TMT) sector, with additional focus on entertainment and data protection. Her expertise includes complex and innovative matters involving new technologies regulation, Over-the-Top (OTT) platforms, and telecommunication services.

Contributed by: Tomás Paiva, Vitor Amorim, Caio Moura and Rebeca Cabral, **Pinheiro Neto Advogados**

Pinheiro Neto Advogados

Rua Hungria, 1100
01455-906
São Paulo
Brazil

Tel: +55 11 3247 8400
Email: tpaiva@pn.com.br
Web: www.pinheironeto.com.br

Brazil's Digital Future: Key Trends, Regulatory Shifts, and Investment Opportunities in Technology, Media and Telecommunications

The Brazilian telecommunications, media and technology (TMT) industry is experiencing a pivotal moment. The country is simultaneously accelerating investments in infrastructure and reshaping the regulatory framework that oversees digital services, platforms, connectivity and emerging technologies. For investors and companies assessing opportunities in Latin America's largest economy, understanding the nuances of this transition is essential.

This article provides an overview of the most significant transformations affecting Brazilian telecom operators, digital infrastructure providers, streaming platforms, internet companies, and technology players.

A new phase of infrastructure growth

Brazil's digital and telecom infrastructure is rapidly expanding. With the rollout of 5G, growth in data-centre development, increased investment in submarine cables, and the rise of private industrial networks, the country is becoming one of the most dynamic markets in the region. At the same time, Brazil's large population and vast geographic scale continue to offer significant opportunities for future growth.

5G deployment and coverage obligations

The commitments established in the 2021 5G spectrum auction have now reached a critical phase of execution. Mobile operators are facing ambitious deadlines, including the requirement to activate "pure" 5G standalone services in hundreds of mid-sized cities. Meeting these obligations demands substantial investment in antennas, fibre backhaul, and core network upgrades.

The expansion into less populated regions also creates significant opportunities for equipment vendors, network builders, tower companies, and neutral-host infrastructure providers.

ANATEL has already signalled that additional spectrum bands will be auctioned in 2026. These upcoming tenders are expected to introduce new coverage obligations and commitments, once again requiring major capital outlays and potentially opening the door for new market entrants.

The rise of private networks

Private networks are rapidly expanding across sectors such as agribusiness, mining, energy, and port logistics. These industries need secure, low-latency, high-availability connectivity to support automation, robotics, and industrial IoT. Some organisations are building their own dedicated networks, while others are partnering with major telecom operators or ISPs. As a result, private networking is becoming a high-value B2B segment, with growth expected to continue as industries adopt AI-driven automation and real-time monitoring systems.

Data centres and submarine cables

Brazil is positioning itself as the most significant data hub in the Southern Hemisphere. Demand for processing power has surged with the expansion of cloud services and the rise of generative AI applications, driving a new wave of hyperscale data-centre developments.

To support this growth, the Federal Government introduced REDATA (Provisional Measure No 1,318/2025), a special tax regime designed to encourage investments in data centres, cloud infrastructure, AI, and high-performance computing. Projects must meet sustainability and innovation criteria to qualify, aligning Brazil with global trends toward greener digital infrastructure. In addition, both federal and local governments are creating special zones dedicated to data centres and subsea cable operations, offering targeted tax benefits.

International connectivity is also expanding. Several new submarine cable systems are under development, aimed at increasing redundancy, reducing latency, and strengthening direct connections between Brazil, Europe, and Africa – ultimately reducing reliance on North American routes.

Together, these initiatives enhance Brazil's digital resilience and reinforce its position as a strategic hub for global data traffic.

Regulatory updates and developments in the spectrum market

ANATEL's upcoming 700 MHz auction

ANATEL is preparing a new auction for the 700 MHz band, a frequency valued for its excellent propagation characteristics and its ability to provide wide-area coverage. This spectrum is strategically important not only for expanding broadband access in rural and remote regions – where deployment costs are typically higher – but also for enhancing service quality in densely populated urban areas.

With demand for mobile connectivity continuing to grow, the auction is expected to draw interest from both established operators and new entrants, though preference is likely to lean toward the regional carriers that acquired 3.5 GHz spectrum in the previous 5G auction. The associated rollout obligations may further encourage investment in equipment, network resources, and supporting infrastructure.

New spectrum regulations and secondary use models

Brazil is updating its spectrum-governance framework to better support emerging technologies and improve the efficiency of radiofrequency use. Following an amendment to the Brazilian Telecommunications Law that allows radio frequencies to be assigned without requiring a service licence, ANATEL is now evaluating regulatory models that enable secondary use of spectrum. This would allow multiple users to operate in the same band under controlled interference conditions.

As part of this effort, ANATEL is considering a "use it or lease it" approach, which could significantly increase spectrum efficiency and foster innovative applications across various sectors. These regulatory developments may also pave the way for dynamic spectrum-sharing models and the deployment of new technologies.

Heightened cybersecurity and certification requirements

Cybersecurity has become a top priority for the Brazilian government and local regulators. As a result, companies that introduce telecommunications equipment or operate digital infrastructure are now subject to stricter rules.

Security-by-design in telecoms equipment

ANATEL has updated its certification and homologation rules to include mandatory cybersecurity requirements grounded in security-by-design principles. Under these rules, manufacturers and importers of telecommunications equipment must carry out technical testing, risk assessments, and audits before their products can be approved for the Brazilian market. As a result, compliance costs are rising, certification timelines are becoming longer, and more detailed technical documentation is required.

Certification expands to data centres linked to telecom networks

A recent regulatory update has expanded ANATEL's certification requirements beyond traditional telecommunications equipment. Under the revised framework for equipment certification and homologation, data centres connected to telecom networks may now also need to meet telecom certification standards. This change will affect cloud providers, colocation operators, and hyperscalers operating in Brazil.

A new liability framework for digital platforms

Brazil's legal framework for internet platforms is undergoing major change. A recent Supreme Court ruling reinterpreted Article 19 of the Brazilian Internet Act, altering liability rules that had been in place for years.

The Supreme Court Decision on Article 19

For nearly a decade, platforms were only liable for third-party content if they failed to comply with a specific court order requiring its removal. The Supreme Court has now adopted a more flexible, risk-based interpretation.

Under this new approach, platforms may incur liability if they do not act proactively against "manifestly illegal" content or if they display systemic failures in moderation. This marks a shift toward a hybrid model that combines traditional notice-and-takedown procedures with proactive monitoring responsibilities.

As a result, companies must strengthen their content governance, enhance detection systems, and increase transparency.

The "Digital ECA" and protection of minors

New legislation aimed at protecting children and adolescents online will take effect in March 2026. Platforms will be required to implement strict privacy-by-default settings and avoid features that encourage excessive or compulsive use. They must also moderate or remove harmful content, including material related to sexual exploitation, violence, cyberbullying, self-harm, gambling, and misleading advertising.

The legislation will prohibit behavioural advertising targeted at minors and will mandate robust age-verification mechanisms. These new obligations will require significant updates to platform architecture, terms of service, and content-moderation practices.

The growing debate over network fees

As internet traffic continues to grow, debates in Brazil over who should fund network expansion have intensified, mirroring similar discussions in Europe. Telecom operators argue that large digital platforms use a disproportionate share of network capacity and should therefore contribute financially.

ANATEL is currently studying whether regulatory intervention is necessary and may propose obligations for value-added services (VAS), since these services are considered users of telecommunications networks. Although ANATEL has ruled out network fees for now, other forms of intervention – such as informational flow requirements or settlement mechanisms – may still be proposed. A public consultation on the matter will open soon.

Changes in media and audiovisual regulation

Digital media consumption continues to transform the audiovisual landscape, and several bills currently under consideration in the Brazilian Congress aim to establish new regulations for streaming platforms and video distribution services.

Streaming regulation and national content quotas

The push for legislation introducing national content quotas and a sector-specific tax on Video-on-Demand (VoD) services is gaining momentum. If adopted, these measures will require platforms to reevaluate their licensing strategies, expand investments in local productions, and adjust their pricing models. Overall, the regulatory landscape for audiovisual services is shifting toward increased oversight and tighter controls.

Transformation of pay-TV and the rise of FAST channels

Traditional pay-TV continues to decline, leading many providers to shift toward IP-based distribution models. At the same time, FAST channels – free, ad-supported streaming channels – are gaining significant traction in Brazil. This trend is creating new revenue opportunities not only for advertisers and content creators but also for technology providers.

TV 3.0: the next frontier

Brazil is preparing to launch TV 3.0, a new broadcasting standard that combines traditional over-the-air television with internet-based interactivity. This technology transforms broadcast TV into an app-like experience, enabling features such as addressable advertising, real-time viewer interaction, and geolocated content delivery.

For investors, TV 3.0 presents opportunities across AdTech, e-commerce integrations, and next-genera-

tion broadcasting equipment. It also has the potential to reshape how open broadcast television competes for advertising budgets.

Cybersecurity and operational resilience as strategic priorities

Cybersecurity is increasingly recognised as a core national security priority. Critical infrastructure sectors now face expanding obligations, including mandatory incident reporting, adherence to technical standards, and stronger oversight of third-party risks.

Organisations are also expected to maintain audit-ready incident response plans and adopt more rigorous risk-management practices. These requirements apply broadly across telecom operators, data centres, cloud providers, and technology companies.

In addition, cyber due diligence has become a crucial element of mergers, acquisitions, and strategic partnerships, as investors place greater emphasis on operational resilience and continuity – not just regulatory compliance.

Satellite connectivity and space sustainability

Satellite technologies in Brazil are entering a new phase, led by low-Earth orbit (LEO) constellations that can deliver high-speed, low-latency broadband across the country. These systems are becoming essential for connecting remote regions, supporting agribusiness operations, and ensuring resilient communications during emergencies. At the same time, Brazil is strengthening its commitment to space sustainability by participating in global efforts related to debris mitigation, orbital traffic management, and responsible satellite operations. As satellite connectivity continues to expand, balancing technological innovation with solid regulatory safeguards will be key to ensuring long-term viability and security in space activities.

Brazil's emerging artificial intelligence framework

Brazil is progressing toward comprehensive AI legislation modelled on the European Union's risk-based approach. The draft law classifies AI systems from "unacceptable risk" to "high risk," with each category carrying specific requirements for transparency, governance, and human oversight. For companies in the TMT sector, this will likely necessitate new internal controls, enhanced documentation processes, and stronger accountability frameworks.

M&A and investment trends in the TMT sector

After a period of global uncertainty, Brazil's M&A market is showing renewed momentum, driven largely by technology-focused transactions. Companies are looking to boost efficiency, accelerate digital transformation initiatives, and expand into new markets.

In particular, Brazil's regional internet service provider (ISP) sector continues to undergo rapid consolidation. Following years of accelerated growth fuelled by extensive fibre-optic deployment and strong local market penetration, many ISPs now face increasing competitive pressure, rising operational costs, and a greater need for scale. These factors have encouraged a wave of M&A activity, with larger players and investment funds acquiring smaller providers to broaden coverage and improve operational efficiency. As consolidation advances, the market is expected to shift toward fewer, stronger groups capable of competing more effectively and supporting advanced services such as cloud connectivity and edge computing.

Conclusion: a strategic inflection point for Brazil's digital economy

Brazil is entering a pivotal phase in the development of its digital ecosystem. Significant investments in large-scale infrastructure, the introduction of new regulatory frameworks, stricter cybersecurity requirements, and the emergence of AI-focused regulation are reshaping the landscape.

For companies and investors, success will depend on understanding how these regulations are evolving, anticipating future compliance obligations, and positioning themselves strategically within the growing digital value chain.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com