Chambers AND PARTNERS

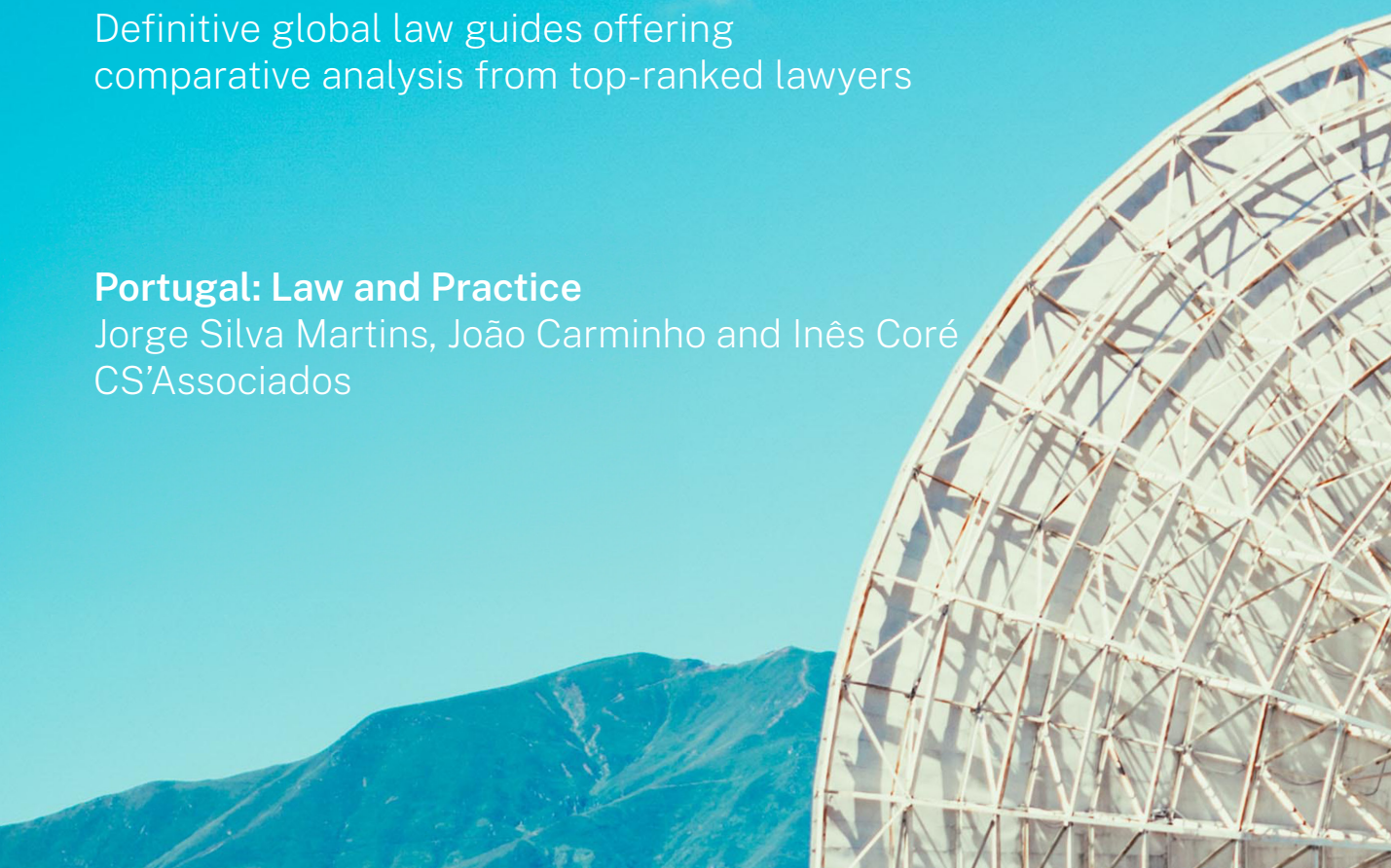
CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2025

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

Portugal: Law and Practice

Jorge Silva Martins, João Carminho and Inês Coré
CS'Associados



PORTUGAL

Law and Practice

Contributed by:
Jorge Silva Martins, João Carminho and Inês Coré
CS'Associados

Contents

CS'Associados is a full-service law firm headquartered in Lisbon, serving national and international clients across different sectors and industries. With a forward-thinking approach, its technology, data and digital innovation practice stands at the forefront of the rapidly evolving TMT landscape. The firm has established a strong reputation for its expertise in key areas such as data protection, electronic communications, e-commerce, internet law, cybersecurity, AI, and intellectual property. The practice area is led by Jorge Silva Martins and is supported by a team of three associates. Recent highlights of the team's work include: (i) providing comprehensive advice to one of the largest global fashion retail brands, and (ii) assisting a global in-flight internet provider with its entry into the national market. In addition, the firm has undertaken significant work involving the negotiation of agreements related to the acquisition of key software products for one of Portugal's largest consumer electronics retailers.

Authors

Jorge Silva Martins leads the technology, data and digital innovation practice area at CS'Associados. With 20 years of experience, primarily in highly regulated sectors, Jorge offers counsel to both national and international companies across sectors. His areas of focus span electronic communications, platform regulation, data protection, internet law, and cybersecurity. In recent years, Jorge has expanded his expertise to include emerging technologies, with a focus on blockchain, and artificial intelligence. He is the author of two books on data protection and Web3, has published several articles in the field of technology, and is a regular speaker at industry and academic conferences.

João Carminho is a managing associate at CS'Associados in the technology, data and digital innovation practice, where he provides tailored legal advice in areas such as electronic communications, e-commerce, privacy and data protection, advertising, consumer law, and intellectual property. João has extensive experience advising technology clients on pre-litigation strategies (often leading negotiations with counterparties) and representing them in dispute resolution before relevant authorities and judicial courts. In addition to his technical expertise, João is recognised for his ability to bridge the gap between complex legal frameworks and business priorities, providing clients with strategic guidance to navigate the fast-paced and ever-evolving technology landscape.

Inês Coré is a senior associate at CS'Associados in the technology, data and digital innovation practice area. She specialises in data protection, intellectual property, and information technology law, providing strategic advice and practical solutions to help clients navigate complex regulatory frameworks. With a focus on fostering compliance in an ever-changing legal environment, Inês works closely with clients to address the challenges posed by technological advancements and innovation. Her expertise ensures that businesses remain agile and well-positioned to meet shifting legal demands, particularly in the areas of digital transformation and data-driven strategies.

CS'Associados

Avenida da Liberdade, 249 – 8.º
1250-143 Lisboa
Portugal

Tel: +351 211 926 800
Email: mailroom@csassociados.pt
Web: www.csassociados.pt/en

CS'ASSOCIADOS

1. Digital Economy

1.1 Key Challenges

Context

The digital economy has transcended its technological roots to become a driving force across all industries and sectors, seamlessly merging the digital and physical worlds. From e-commerce platforms reshaping traditional retail to IoT devices revolutionising manufacturing and logistics, digital innovation is no longer confined to a single domain – it permeates every aspect of business and society.

This convergence of the digital and physical has created unprecedented opportunities, but also complex challenges. Companies must navigate issues such as data privacy, cybersecurity, intellectual property, and regulatory compliance, all while adapting to rapid technological advancements and heightened consumer expectations – in terms of diversity of products/services and in terms of respect of their fundamental rights.

In this "brave new" digital economy, understanding the interplay between legal frameworks and business strategy (and risks) is essential for companies to become and remain competitive.

Portugal

Portugal's regulation of the digital economy is closely aligned with the EU's robust legal framework, ensuring consistency with EU-wide initiatives while fostering national innovation.

Although foundational "first generation" regimes, such as Decree-Law No 7/2004 (transposing into national law the 2000 EU e-Commerce Directive), continue to play a pivotal role in Portugal digital ecosystem, the legal landscape has undergone profound transformation. This evolution is mostly driven by the implementation of the two digital agendas for Europe (2010/2020 and 2020/2030), the Digital Single Market Strategy, and targeted programmes to accelerate the development of advanced technologies.

Among the significant legislative regimes recently adopted in Portugal's digital space, the following stand out:

- Law No 46/2018, establishing the cybersecurity legal framework, transposing Directive (EU) 2016/1148 (NIS Directive);
- Law No 58/2019, implementing the General Data Protection Regulation;
- Decree-Law No 12/2021, implementing Regulation (EU) 910/2014 (eIDAS Regulation), governing electronic identification and trust services for electronic transactions in the internal market;
- Law No 27/2021, which approves the Portuguese Charter on Human Rights in the Digital Age;
- Decree-Law No 65/2021, regulating the cybersecurity legal framework and establishing cybersecurity certification obligations under Regulation (EU) 2019/881;
- Decree-Law No 84/2021, which regulates consumer rights in the purchase and sale of digital goods, content and services, transposing Directives (EU) 2019/771 on certain aspects concerning contracts for the sale of goods, and (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services; and
- Law No 16/2022, which approves the new Electronic Communications Law, transposing Directives 98/84/EE, 2002/77/EC and (EU) 2018/1972.

At a political level, Portugal has further demonstrated its commitment to digital transformation. Reflecting this commitment, the govern-

ment approved the Resolution of the Council of Ministers No 207/2024 on 30 December 2024, which establishes the country's National Digital Strategy.

This strategy seeks to accelerate the digitalisation of public and private sectors while fostering inclusivity, innovation, and sustainability. Its core pillars include:

- Public Services Digitalisation: streamlining access to and delivery of public services through advanced digital platforms;
- Economic Digital Transformation: supporting businesses, especially SMEs, in adopting digital tools and transitioning to Industry 4.0;
- Cybersecurity and Data Protection: strengthening digital resilience and compliance with EU data protection regulations;
- Digital Inclusion: bridging the digital divide by promoting digital literacy and ensuring equitable access to digital tools and infrastructure; and
- Green and Digital Transition: encouraging environmentally sustainable digital practices.

This strategic roadmap underscores Portugal's ambition to position itself as a leader in digital innovation in Europe, aligned with EU priorities and objectives.

Main Challenges

As the digital economy continues to evolve, new challenges emerge, demanding innovative solutions and adaptive policies. Portugal, like many countries, faces a range of pressing issues, among which the following stand out:

- Artificial Intelligence Regulation: The integration of AI across industries raises concerns about ethical use, accountability and transparency. Policymakers must balance fostering innovation with ensuring AI systems are fair, non-discriminatory, and safe.
- Cybersecurity Threats: As digital infrastructure becomes more interconnected, cyber-attacks grow in sophistication and scale. Protecting critical systems, businesses, and consumers requires significant investments in cybersecurity measures and international co-operation.
- Cross-Border Data Flows: The growing importance of data for global trade presents challenges in ensuring compliance with differing international data protection laws while maintaining competitiveness in a data-driven economy.
- Digital Inclusion: Despite advancements, access to digital tools, services, and skills remains unequal. Addressing digital divides, particularly for older generations, low-income populations, and rural areas, is critical to creating an inclusive digital economy.

1.2 Digital Economy Taxation

In Portugal, the taxation of digital services and goods is governed by the European Union's VAT system, as Portugal is an EU member state. Consequently, national tax laws are regularly updated to reflect EU directives, including VAT reforms and digital taxation rules.

However, the dynamic and complex nature of the digital economy presents challenges for businesses, particularly emerging companies offering digital services. Common issues include accurately determining the customer's location and applying the correct VAT rate, which can be particularly problematic for non-resident entities.

Additionally, while the One-Stop-Shop (OSS) system and VAT registration processes are intended to streamline compliance, they often remain administratively demanding. Uncertainty

and ambiguity in the interpretation and practical application of tax regulations can create further uncertainty.

1.3 Taxation of Digital Advertising

As a member state of the EU, Portugal's taxation of digital advertising revenues is governed by the European Union's rules, ensuring alignments with broader EU directives. The tax implications for such revenues depend on several factors, including the type of entity earning the revenue (resident or non-resident), the nature of the transaction (B2B or B2C), and the applicable Portuguese tax laws.

To ensure compliance with Portuguese tax requirements for digital advertising revenues, companies can adopt several best practices, including:

- Leverage tax compliance software: automate VAT calculations, invoicing, and reporting using software compatible with Portuguese requirements;
- Ensure SAF-T compliance: configure accounting systems to produce the Standard Audit File for Tax (SAF-T), which is required for audits and e-invoicing compliance:
- Maintain accurate customer data: collect and maintain precise information on customer location and VAT status to determine applicable tax obligations; and
- Keep comprehensive records: retain detailed documentation of transactions, including invoices, contracts, and tax filings, to meet audit and compliance requirements.

1.4 Consumer Protection

As digital goods and services increasingly dominate the TMT sector, robust consumer protection frameworks have become critical to ensuring transparency, fairness, and trust in the digital marketplace. In Portugal, a combination of EU regulations and national laws creates a comprehensive legal framework, addressing consumer protection from multiple perspectives within the digital environment. Key legislation includes:

- Law No 24/96 (Consumer Protection Law);
- Decree-Law No 7/2004 (on certain legal aspects of information society services, in particular electronic commerce, in the internal market);
- Law No 41/2004 (on the processing of personal data and privacy protection in electronic communications);
- Decree-Law No 57/2008 (applicable to unfair commercial practices);
- Decree-Law No 166/2013 (applicable to individual restrictive trade practices);
- Decree-Law No 24/2014 (applicable to on distance and off-premises contracts);
- Regulation (EU) 2016/679 (General Data Protection Regulation);
- Law No 58/2019 (implementing the GDPR in Portugal);
- Decree-Law No 84/2021 (which sets out the rights of consumers in case of lack of conformity of digital goods, content or services); and
- Regulation (EU) 2022/2065 (Digital Services Act).

Companies operating in the digital economy play a critical role in upholding consumer rights. By adopting the following measures, they can enhance compliance with legal frameworks and foster trust among their consumers:

- Transparency: clearly inform consumers about their rights, terms and conditions, and how their data will be processed, in accordance with the GDPR and consumer protection laws;

- Fair contracts: draft digital contracts that are fair and free from unfair or imbalanced clauses;
- Secure transactions: implement robust security measures to safeguard consumer data and ensure safe online transactions, which are essential for maintaining trust and complying with data protection regulations; and
- Customer support: provide accessible and responsive customer service channels for handling consumer complaints, inquiries, and dispute resolution.

The resolution of consumer disputes in the digital economy is guided by the Consumer Protection Law and other related regulations. Disputes of low economic value (up to EUR5,000.00) are subject to mandatory arbitration or mediation if the consumer expressly chooses to submit the matter to an arbitration court attached to legally authorised consumer dispute arbitration centres.

For disputes of up to EUR15,000.00, the "*julgados de paz*" (extrajudicial courts) can also play a significant role, provided they are territorially competent. For disputes exceeding this threshold, the general civil procedural law applies, and ordinary civil courts have jurisdiction.

To effectively manage consumer disputes, TMT companies must ensure strict compliance with the legal standards outlined in the relevant laws (listed above), particularly regarding transparency, fairness, and the avoidance of unfair contractual clauses. Additionally, they should establish efficient internal communication and consumer-focused dispute resolution channels. By fostering the use of out-of-court dispute resolution mechanisms, companies can minimise reliance on formal court proceedings, thereby reducing the associated time, costs, and complexities, while enhancing consumer trust.

1.5 The Role of Blockchain in the Digital Economy

Blockchain technology is revolutionising the digital economy, offering a decentralised and secure mechanism to manage transactions, data, and processes across various industries. In the TMT sector, blockchain has emerged as a transformative tool, driving transparency, reducing reliance on intermediaries, and enabling faster, more efficient operations. While cryptocurrencies remain one of its most recognisable applications, blockchain's potential extends far beyond digital currencies, creating significant opportunities for innovation and growth.

Blockchain technology offers transformative potential, but its adoption is not without challenges. One key issue is regulatory uncertainty. Despite substantial progress in certain areas (mainly due to the anti-money laundering regime and MiCA), ambiguity remains around the classification of cryptocurrencies and tokens, particularly regarding their compliance with securities laws and licensing requirements. This lack of clarity creates hurdles for businesses seeking to innovate within a secure and compliant legal framework.

Additionally, blockchain's pseudonymity introduces significant risks related to anti-money laundering (AML) and counter-terrorism financing (CTF). Businesses operating in this space must implement robust due diligence measures to mitigate these risks and adhere to legal obligations. Another challenge lies in reconciling blockchain's inherent transparency and immutability with the requirements of the General Data Protection Regulation.

Blockchain and cryptocurrency activities in Portugal are increasingly subject to regulatory oversight, creating a structured framework for their

use and development. Key aspects of the legal landscape include, without limitation, taxation, AML requirements, and securities regulation:

- Taxation: The State Budget Law for 2023 introduced a tax regime for cryptocurrency transactions, bringing greater clarity to this area. For individuals, gains from cryptocurrency transactions are taxed at a flat rate of 28%, unless the cryptocurrency is held for more than a year, in which case the gains are tax-exempt. For businesses, cryptocurrency transactions are subject to corporate income tax as part of their taxable revenue.
- Anti-money laundering: Under Law No 83/2017 (which establishes measures to combat money laundering and terrorism financing), companies engaged in virtual asset activities (as defined in this regime) must comply with stringent AML and CTF regulations. These include mandatory registration with Banco de Portugal, the supervisory authority for such entities.
- Securities regulation: Initial Coin Offerings (ICOs), Security Token Offerings (STOs), and other token-based financing mechanisms may fall under Portuguese securities laws (particularly, the Portuguese Securities Code, approved by Decree-Law No 486/99), depending on the specific characteristics of the tokens issued. In Portugal, compliance with these regulations is overseen by the Portuguese Securities Market Commission (CMVM), which ensures that issuers meet the necessary legal requirements for investor protection and market transparency.

By implementing these regulatory measures, Portugal is positioning itself as a forward-thinking jurisdiction for blockchain and cryptocurrency activities. These frameworks not only promote legal certainty but also foster innovation and trust in the use of blockchain technologies in the digital economy.

2. Cloud and Edge Computing

2.1 Highly Regulated Industries and Data Protection

In Portugal, cloud and edge computing, as they fundamentally involve data processing, are primarily regulated by the General Data Protection Regulation, along with national legislation. The GDPR establishes rules governing the protection and free movement of personal data, imposing obligations on entities processing personal data, including cloud and edge computing service providers. Key requirements focus on security of processing, obligations for data processors, and the transfer of personal data to third countries.

At the national level, Law No 46/2018 establishes Portugal's cybersecurity framework, transposing Directive (EU) 2016/1148 (NIS Directive) on network and information security. This law imposes security requirements on operators of essential services and digital service providers, including cloud computing providers. Additionally, Law No 58/2019 implements the GDPR in Portugal, providing further guidance on compliance with data protection laws. The Portuguese Data Protection Authority (CNPD) has also issued Guideline No 2023/1, which details organisational and security measures applicable to the processing of personal data.

Certain regulated industries, particularly those handling large volumes of sensitive data, are subject to stricter security and compliance requirements. These include sectors such as banking, insurance, healthcare, finance, and telecommunications, which must implement

higher security standards and additional regulatory safeguards.

Cloud computing raises significant legal concerns regarding security, data transfers, and the role of cloud providers in personal data processing. A major issue is that cloud providers often act as processors under the GDPR, meaning they process data on behalf of controllers and must comply with Article 28 of the GDPR, which imposes contractual obligations to ensure data security and regulatory compliance. Controllers must verify that cloud providers implement robust security measures, access controls, and breach response mechanisms.

3. Artificial Intelligence

3.1 Liability, Data Protection, IP and Fundamental Rights

Portugal does not yet have specific national legislation dedicated to AI. However, as an EU member state, it is subject to all EU regulatory initiatives in this field, particularly the AI Act, which applies in Portugal and serves as the primary legal framework for AI.

Under the AI Act, however, member states must adopt an implementing act by 2 August 2025, which will establish, among other provisions, rules on penalties, including administrative fines.

To comply with Article 77 of the AI Act, Portugal has designated 14 national authorities responsible for overseeing compliance with EU fundamental rights legislation in the use of high-risk AI systems. Among them, ANACOM has been assigned the role of co-ordinating efforts among all designated authorities.

Beyond the AI Act, Portugal's AI regulatory landscape encompasses both horizontal and sector-specific regulations at the national and EU levels, including, but not limited to, consumer protection laws and privacy and data protection regimes (particularly, the GDPR).

Although not a legislative instrument, the Portuguese Charter on Human Rights in the Digital Age (Law No 27/2021) is also relevant. The Charter emphasises ethical principles such as transparency, accountability, and non-discrimination in the design and application of AI and robotics, as outlined in Article 9.

With regards to deepfake technologies, Portugal has not yet introduced legislation addressing this specific use of technology. However, existing laws provide legal safeguards against the unauthorised use or manipulation of an individual's likeness and voice:

- The Portuguese Civil Code protects individuals against unauthorised use of their image and voice, meaning that creating or distributing without consent may constitute a violation of personality rights.
- The Portugal Penal Code includes provisions on defamation and offences against a person's honour, which may apply to the malicious use of deepfake technology.
- The GDPR, applicable across the EU, also provides protection by regulating the processing of personal data, including visual and audio data used in deepfakes.

Finally, Portugal has yet to implement specific legislation for AI application in the transport sector, such as self-driving cars and/or drones. However, existing national and EU regulations provide a foundational legal framework:

- Self-driving cars: The Portuguese Highway Code (approved by Decree-Law No 114/94) has not been updated to address autonomous vehicles. However, pilot projects and tests for self-driving cars fall under EU regulations, particularly the Vehicle General Safety Regulation (Regulation (EU) 2019/2144), which establishes safety and liability standards.
- Commercial drones and drone delivery services: Drone operations in Portugal are governed by Regulation (EU) 2018/1139, and the EU Drone Regulation (Regulations 2019/945 and 2019/947). These have been implemented nationally through Decree-Law No 87/2021, with ANAC (the National Civil Aviation Authority) responsible for enforcement.

4. Internet of Things

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

Machine-to-Machine Communications

Portugal does not yet have specific legislation governing IoT. However, as a EU member state, it is subject to the EU regulatory initiatives that shape the legal framework for IoT.

Since IoT relies heavily on data processing to enable Machine-to-Machine Communications, its regulation falls under the broader EU data governance framework, including:

- the GDPR (Regulation (EU) 2016/679);
- the Data Act (Regulation (EU) 2023/2854); and
- the Data Governance Act (Regulation (EU) 2022/868).

IoT technologies pose significant data protection risks, as smart devices (eg, wearables) frequently collect personal data, including special categories of data, such as health information (Article 9 of the GDPR). The ability to collect, process and combine datasets enables smart objects to enhance performance and user experience. However, this also raises concerns about data security and potential personal data breaches (Article 4(12) of the GDPR) due to unauthorised access or cybersecurity threats.

The Data Act regulates data generated by user-connected products on public electronic communications networks. It aims to harmonise rules on fair data access and usage, clarifying who can create value from data and under what conditions – a crucial aspect for IoT, as smart devices rely extensively on user-generated data.

The Data Governance Act focuses on data-sharing frameworks, regulating processes and structures to facilitate such exchange of information.

The EU Cyber Resilience Act (Regulation 2024/2847) is also critical for IoT as it establishes essential cybersecurity requirements for connected devices, ensuring stronger protection against cybersecurity threats. With billions of interconnected IoT devices – from smart home systems to industrial sensors – the risk of cyberattacks that could compromise data privacy, disrupt critical services, or endanger safety is significantly increased. The Cyber Resilience Act enforces security by design, requiring manufacturers to implement robust cybersecurity measures throughout a product's lifecycle, including regular updates and vulnerability management.

Communications Secrecy

Communications secrecy in the context of IoT technologies is governed by broader regulations on data protection, cybersecurity, and consumer rights.

In addition to the GDPR, which provides general protection for personal data, the ePrivacy Directive (Directive 2002/58/EC) specifically regulates privacy in electronic communications, serving as lex specialis in relation to the GDPR. While the ePrivacy Directive remains in force, a new ePrivacy Regulation is under discussion and is expected to update and strengthen privacy rules for electronic communications, including IoT devices.

The NIS2 Directive (Directive (EU) 2022/2555) which entered into force on 16 January 2023, replacing its predecessor, the NIS Directive, is considered the EU's primary cybersecurity legislation. While it does not explicitly regulate IoT, it has broader cybersecurity implications for cybersecurity, indirectly impacting communication secrecy within IoT ecosystems. Portugal is expected to complete the transposition of the NIS2 Directive into national law soon.

Additionally, recognising the security risks posed by products with digital elements, including IoT technologies, the European Commission adopted the Cyber Resilience Act – which establishes comprehensive cybersecurity standards for connected devices.

4.2 Compliance and Governance

Compliance Challenges

Companies deploying IoT solutions in Portugal need to deal with several compliance challenges, primarily related to data protection and cybersecurity:

- Data protection obligations:
  - (a) IoT devices often collect vast amounts of personal data, triggering compliance requirements under the GDPR. Key challenges include ensuring transparency, obtaining valid consent from data subjects, and adhering to the principles of data minimisation and purpose limitation.
  - (b) Companies must also address the complexities of IoT data security, particularly given the potential vulnerabilities in connected environments.
- Cybersecurity concerns:
  - (a) IoT devices are often considered weak entry points for cyberattacks, increasing the need for companies to ensure proper encryption, secure firmware updates, and vulnerability management.
  - (b) Operators of Essential Services (OES) under the NIS Directive (as implemented in Portugal) face stricter obligations if IoT solutions are integrated into critical infrastructure.
- Interoperability and standards: The fragmented IoT ecosystem presents challenges in ensuring compliance with technical standards, particularly when integrating devices from multiple manufacturers.

Governance Frameworks for IoT Deployments

To ensure effective IoT deployment and regulatory compliance, companies in Portugal should adopt governance frameworks tailored to the risks and legal requirements associated with IoT technologies:

- Data protection governance:
  - (a) establish a Data Protection Impact Assessment (DPIA) process to evaluate risks related to personal data processing, as required under the GDPR for high-risk processing; and
  - (b) appoint a Data Protection Officer (DPO) to oversee IoT-related data protection compliance, particularly for organisations processing large-scale or sensitive personal data.

- Cybersecurity governance:
  (a) implement a Cybersecurity Management System aligned with standards such as ISO/IEC 27001 and ENISA guidelines for IoT security; and
  (b) conduct regular vulnerability assessments and penetration testing to identify and mitigate risks associated with IoT devices.
- IoT-specific policies and controls:
  (a) develop governance policies for IoT deployments, covering areas such as device authentication, encryption standards, and data lifecycle management; and
  (b) establish clear guidelines for third-party IoT vendors, ensuring compliance with Portuguese and EU data protection and cybersecurity laws.

4.3 Data Sharing

Key Legal Requirements

IoT companies in Portugal must comply with the following key legal requirements regarding data sharing:

- General Data Protection Regulation (GDPR):
  (a) Personal data sharing must align with GDPR principles, including lawfulness, fairness, transparency, purpose limitation, and data minimisation.
  (b) Processing personal data requires a valid legal basis (eg, user consent or legitimate interests), and users must be clearly informed about how their data will be shared and for what purpose.
- Data Act (Regulation (EU) 2023/2854): The Data Act introduces additional obligations for IoT manufacturers and service providers to facilitate access to and the sharing of data generated by connected devices. Key requirements include:
  (a) User empowerment: Users (individuals or businesses) must be able to access and share the data generated by their IoT devices with third parties of their choice;
  (b) Fair, reasonable, and non-discriminatory (FRAND) terms: Data-sharing agreements, particularly in B2B contexts, must adhere to FRAND principles.
  (c) Business-to-government (B2G) sharing: IoT companies may be required to share data with public authorities in cases of emergencies or public interest needs.
- Sector-specific rules: Certain industries, such as healthcare, finance, and energy, are subject to heightened data-sharing requirements due to their reliance on high-value or sensitive data.

Heightened Requirements for Specific Data Categories

- Special categories of personal data: GDPR imposes stricter requirements for processing and sharing special categories of data (eg, health data, biometric data) generated by IoT devices.
- Trade secrets and proprietary data: The Data Act protects trade secrets and ensures that data sharing does not undermine a company's intellectual property, provided confidentiality safeguards are applied.

5. Audiovisual Media Services

5.1 Requirements and Authorisation Procedures

Provision of Audio–Visual Media Services in Portugal

The provision of audio–visual media services (AVMS) in Portugal is primarily governed by the following legislation:

- Decree-Law No 46/2023 (which transposes into national law Directive (EU) 2019/789

laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasters and the retransmission of television and radio programmes);
- Decree-Law No 47/2023 (which transposes into national law Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market or "CDSM Directive");
- Decree-Law No 82/2022 (which transposes into national law Directive (EU) 2019/882 on Accessibility Requirements for Products and Services or "European Accessibility Act");
- Law No 74/2020 (which transposes into national law Directive (EU) 2018/1808, amending Directive 2010/13/EU or "Audiovisual Media Services Directive"); and
- Law No 27/2007, as amended (which approves the television law, transposing into national law Directive 97/36/EC).

Under the applicable legal framework, AVMS in Portugal may be provided by the following operators:

- television services broadcasters;
- providers of on-demand audio–visual services; and
- video-sharing platform services made available in the Portuguese territory by video-sharing platform providers.

The above-mentioned legal regimes impose various requirements that must be met transversally by AVMS providers. However, stricter rules apply to television broadcasting, particularly in advertising and the protection of minors, due to its great societal impact.

According to the Portuguese AVMS Law, AVMS providers must ensure that their programming respects fundamental rights, and does not (i) provoke or incite violence or hatred against any group (eg, minorities), and (ii) encourage the commission of terrorist offences.

Moreover, television service broadcasters are subject to specific restrictions not only concerning content but also regarding the applicable timeframes for making such content available. This particularly applies to content that is likely to be harmful to minors and could adversely affect the development of their personality. Such content may only be aired between 10 pm and 6am, and must display a visual warning symbol throughout its duration.

The same applies to on-demand audio-visual service providers, who must similarly identify and label such content and provide technical parental control features to restrict minors' access.

With regard to advertising, television commercials and teleshopping aired from 6am to 6pm, as well as from 6pm to midnight, must not exceed 10% or 20%, depending on whether they pertain to conditional access television programme services or free/conditional access television programme services with a subscription.

Video-Sharing Platforms

Certain content restrictions applicable to television and on-demand AVMS providers also extend to video-sharing platform services. These obligations primarily focus on protecting minors and the public from hate speech and incitement to violence, as well as other forms of hateful content, including criminal and child pornographic material. Therefore, video-sharing platforms must moderate user-generated content to a certain extent to ensure compliance with these obligations.

Moreover, following the entry into force of the Digital Services Act (Regulation (EU) 2022/2065), video-sharing platforms must also comply with stricter measures to combat illegal content online.

Administrative Proceedings

Under Article 13 of the Portuguese AVMS Law, television activities require a licence if they use terrestrial radio spectrum for broadcasting. Licensing is granted through a public tender initiated by the government and applies to:

- organising unconditional access television programme services; and
- selecting and aggregating television programme services with conditional access or subscription-based access.

If television activities do not use terrestrial radio spectrum and are instead distributed through a licensed operator, only a mere authorisation is required.

Television services broadcasters, on-demand AVMS providers, and video-sharing platform providers are subject to registration with the ERC, the Portuguese Regulatory Authority for the Media.

6. Telecommunications

6.1 Scope of Regulation and Pre-Marketing Requirements

The Scope of Local Regulation

Under the Portuguese Electronic Communications Law (Law No 16/2022), which transposes the European Electronic Communications Code (EECC) into national law, the scope of local telecommunications rules has been broadened to reflect technological advancements and market developments. In this regard, the law applies to the following technologies and services:

- traditional telecommunication services (fixed and mobile voice services, internet access services, and transmission services used for broadcasting);
- interpersonal communication services and number-independent interpersonal communication services;
- Machine-to-Machine (M2M) and Internet of Things (IoT);
- private and business communication networks;
- satellite and space-based communication services (including low-earth orbit satellite internet services and earth-station services that enable connectivity via satellites); and
- emergency communication and public warning systems.

Pre-Marketing Requirements

The provision of electronic communications networks or services is subject to a harmonised general authorisation procedure before ANACOM. Under this regime, individuals or companies intending to offer publicly accessible or private electronic communications networks and services must notify ANACOM before introducing these services to the market. However, specific licences, such as administrative authorisations required by municipalities, may still be necessary.

In accordance with the general authorisation framework, companies must submit the following information.

- comprehensive company identification, including the company's website associated with the provision of publicly available

electronic communications networks and services;
- communication and notification contacts;
- a concise description of the network or service to be provided, detailing (i) the type of network or service type; (ii) the target market (wholesale or retail); (iii) the supporting network infrastructure; (iv) the key network characteristics and intended purpose; (v) whether numbering or frequency resources are required, along with a specification of such resources;, and (vi) a general description of the service offering; and
- the anticipated commencement date of operations.

Additionally, individual licences are required for the use of numbering and frequency resources.

Security Requirements

Under Portuguese electronic communications laws, particularly Law 16/2022, telecommunications service providers are subject to strict security requirements to ensure the integrity, availability, and confidentiality of their networks and services. These obligations aim to mitigate risks associated with cybersecurity threats, system failures, and other vulnerabilities that could impact service continuity or user security.

Providers of public electronic communications networks and services must implement appropriate technical and organisational measures to manage security risks. These include ensuring network resilience, maintaining service continuity in the event of disruptions, and protecting against cybersecurity threats such as hacking, malware, and denial-of-service attacks. The measures adopted must be proportionate to the risks identified, considering technological advancements and sector best practices.

In the event of a significant security breach or service disruption, providers are required to notify ANACOM, the national regulatory authority, without undue delay. If an incident poses a broader cybersecurity risk to national infrastructure, notification must also be made to the National Cybersecurity Centre (CNCS). Furthermore, if a security incident affects users' personal data or service availability, providers may be required to inform affected customers and advise them on mitigation measures.

The security framework is further detailed in ANACOM's Regulation 303/2019, which establishes specific security and integrity obligations for electronic communications networks and services. This regulation requires operators to assess security risks, define mitigation measures, and submit periodic security reports to ANACOM. It also sets criteria for incident classification, determining which events must be reported based on their impact on service availability, confidentiality, and user protection.

Failure to comply with security obligations can result in administrative fines imposed by ANACOM. Repeated violations or serious negligence in protecting networks and services may lead to operational restrictions or, in extreme cases, the revocation of a provider's licence to operate.

6.2 Net Neutrality Regulations

Key Rules and Principles

In Portugal, net neutrality is primarily governed by EU law, particularly Regulation (EU) 2015/2120, which establishes open internet access rules across the European Union.

Key aspects of net neutrality in Portugal include:

- No blocking or throttling: ISPs may not block, slow down, or discriminate against lawful

content, applications, or services, except when necessary for network security, congestion management, or legal compliance.
- Traffic management rules: Any traffic management practices must be transparent, non-discriminatory, and proportionate.
- Zero-rating practices: Portugal attracted international attention in 2017 when certain ISPs introduced "zero-rating" services, allowing specific applications to be used without consuming data allowances. While this practice raised concerns about potential net neutrality violations, BEREC has issued guidelines stating that zero-rating must not result in discrimination against other services.
- ANACOM monitors compliance with net neutrality rules and has the authority to investigate ISPs suspected of breaching open internet principles.

Impact on the Telecommunications Sector

Net neutrality regulations ensure a level playing field by preventing ISPs from prioritising or restricting specific services based on commercial interests.

While these rules promote consumer rights and fair competition, they also impose operational and financial constraints on ISPs, limiting their ability to develop differentiated service offerings or enter into exclusive agreements with content providers. Compliance with these rules requires continuous regulatory oversight and adaptation to evolving EU guidelines.

6.3 Emerging Technologies

Impact on the Legal Landscape

Emerging technologies such as 5G, IoT, and AI are transforming the telecommunications sector in Portugal, introducing new opportunities and regulatory challenges.

5G deployment

5G technology introduces higher-speed connectivity, lower latency, and increased network capacity, enabling advanced applications such as smart cities, autonomous vehicles, and industrial automation. However, its deployment raises several legal considerations:

- Spectrum allocation and licensing: ANACOM oversees the allocation of 5G spectrum licences, ensuring compliance with EU rules on fair competition and efficient spectrum use. Portugal has already auctioned spectrum in the 700 MHz, 3.6 GHz, and 26 GHz bands, with regulatory obligations for nationwide coverage, particularly in underserved areas.
- Network security and cybersecurity risks: Given the critical infrastructure nature of 5G networks, EU cybersecurity regulations, such as the Cybersecurity Act (Regulation (EU) 2019/881) and the EU Toolbox for 5G Security, impose strict security requirements. Portugal follows these frameworks to mitigate risks related to foreign vendors, cyberattacks, and personal data breaches.

IoT expansion

IoT enables interconnected devices across sectors such as healthcare, transportation, and manufacturing. However, its rapid expansion raises legal challenges in data governance, liability, and cybersecurity:

- Data protection and privacy: The GDPR applies to IoT devices that collect and process personal data. Portugal's National Data Protection Commission (CNPD) enforces GDPR compliance, particularly concerning user consent, data security, and accountability of IoT service providers.
- Liability and consumer protection: The EU Product Liability Directive (85/374/EEC) and

proposed AI Liability Directive introduce new considerations for liability in cases of IoT device malfunctions, especially when AI-driven automation is involved. Service providers and manufacturers must establish clear responsibility frameworks in case of failures.
- Interoperability and standardisation: The EU promotes common technical standards for IoT devices to ensure seamless integration and prevent fragmentation of digital markets. Compliance with the EU Radio Equipment Directive (2014/53/EU) is required for IoT device certification in Portugal.

AI integration

AI is increasingly used in network management, predictive maintenance, chatbots, fraud detection, and personalised services. While AI improves efficiency, it also raises regulatory concerns:

- AI governance and transparency: The upcoming EU Artificial Intelligence Act (AI Act) will regulate AI applications, particularly high-risk AI systems used in telecommunications. Compliance with transparency, explainability, and non-discrimination principles will be mandatory for telecom providers using AI-driven automation.
- Automated decision-making and consumer rights: Under the GDPR, telecom operators using AI for automated decision-making (eg, billing, service recommendations, or fraud detection) must ensure transparency and allow users to contest decisions.

Key Legal Considerations for Companies

Companies in the TMT sector integrating 5G, IoT, and AI must navigate a complex legal framework, particularly in the areas of data protection, cybersecurity, AI governance, competition law, and consumer rights.

The GDPR imposes strict obligations on companies handling personal data, requiring lawful processing, transparency, and data security measures. Given the vast amounts of data processed by IoT devices and AI-driven systems, compliance with user consent, data minimisation, and cross-border transfer rules is critical.

In parallel, the NIS2 Directive and Cybersecurity Act mandate robust network security measures for telecom providers and digital service operators, ensuring resilience against cybersecurity threats, especially in 5G infrastructure and IoT ecosystems.

The EU AI Act introduces a risk-based framework, imposing stringent compliance, transparency, and accountability requirements on AI systems used in telecommunications, such as automated customer service, fraud detection, and network optimisation. Companies must also consider liability risks, as the proposed AI Liability Directive seeks to establish clearer legal accountability for harm caused by AI-driven decisions. In the competition law space, the Digital Markets Act (DMA) and EU antitrust rules (Articles 101 and 102 TFEU) regulate market dominance, data access, and interoperability, preventing unfair restrictions on competitors, particularly in 5G partnerships and IoT data sharing.

Consumer protection laws, including the DSA and Consumer Rights Directive, require TMT companies to ensure fair commercial practices, contract transparency, and dispute resolution mechanisms. For AI-powered services and IoT products, clear disclosures on data collection, software updates, and algorithmic decision-making are essential to avoid regulatory scrutiny.

7. Challenges with Technology Agreements

7.1 Legal Framework Challenges

Challenges

While not unique to Portugal, the challenges associated with technology agreements in the country reflect broader issues faced by organisations across the EU. Businesses entering into such agreements in Portugal must navigate a range of legal, regulatory, and commercial complexities.

Some of the key challenges include:

- Data privacy and security concerns: With increasing emphasis on data privacy and security, technology agreements must incorporate stringent privacy and security provisions. This is particularly critical in highly regulated sectors – such as healthcare, banking and finance, telecommunications, and insurance – where compliance with strict data security standards is mandatory.
- Cross-border operations and jurisdictional issues: Technology agreements involving parties from different jurisdictions often encounter legal and regulatory discrepancies. Establishing the applicable laws and dispute resolution mechanisms requires careful negotiation to mitigate jurisdictional uncertainties.
- Performance and service level compliance: Defining and enforcing performance standards in service level agreements (SLAs) can be complex. Ensuring compliance with agreed-upon service levels necessitates continuous monitoring and, where necessary, contractual adjustments to maintain operational efficiency.
- Cybersecurity vulnerabilities: As technological interconnectivity increases, so does exposure to cybersecurity threats. Technology agreements must incorporate robust cybersecurity measures, incident response protocols, and liability provisions to address potential breaches and mitigate associated risks.

Portugal does not have a specific legal regime governing technology agreements. Instead, these contracts are generally regulated by broader principles of private law, primarily under the Civil Code and the Commercial Code.

In addition to these general legal frameworks, several specific legislative instruments are particularly relevant in this context:

- Law No 58/2019, which ensures the implementation, in the national legal order, of the GDPR;
- Decree-Law No 63/85, which approves the copyright and related rights code;
- Decree-Law No 252/94, concerning the legal protection of computer programs, transposing Council Directive 91/250/EEC;
- Decree-Law No 122/2000, on the legal protection of databases, transposing Directive 96/9/EC, of the European Parliament and of the Council, of 11 March 1996; and
- Decree-Law No 446/85, which approves the Standard Contractual Clauses Regime.

7.2 Service Agreements and Interconnection Agreements

Key Elements of Telecommunications Service Agreements

- Scope of services: clearly define the type of services (eg, broadband, mobile, or voice) and performance standards;
- Service levels (SLAs) and performance metrics: include measurable SLAs, penalties for non-compliance, and provisions for service continuity;

- Data protection: ensure compliance with the GDPR, particularly regarding user data collection, processing, and sharing;
- Pricing and billing: transparent pricing structures, billing mechanisms, and any applicable regulatory pricing controls; and
- Termination and dispute resolution: define conditions for termination and include mechanisms for resolving disputes, such as mediation or arbitration.

Negotiating Favourable Terms

- Flexibility: seek terms that allow adaptation to evolving technologies or regulatory changes (eg, 5G or IoT deployment);
- Risk mitigation: include robust indemnity clauses to limit liability for service outages or data breaches; and
- Regulatory compliance: ensure adherence to national and EU telecom regulations to avoid penalties.

Considerations for Interconnection Agreements

- Regulatory compliance: agreements must comply with Portuguese Electronic Communications Law interconnection regime and EU rules under the European Electronic Communications Code (EECC);
- Technical specifications: clearly define interconnection points, quality standards, and interoperability requirements;
- Cost sharing: establish fair cost allocation for shared infrastructure and services, considering regulated pricing;
- Dispute resolution: include clear procedures for resolving conflicts, as interconnection disputes are subject to ANACOM's oversight; and
- Data and security: address data traffic management, cybersecurity requirements, and privacy obligations.

8. Trust Services and Digital Entities

8.1 Trust Services and Electronic Signatures/Digital Identity Schemes

In Portugal, this topic is governed by Decree-Law No 12/2021, which:

- ensures the implementation within the Portuguese legal order of the eIDAS Regulation;
- regulates the validity, effectiveness and probative value of electronic documents;
- establishes the recognition and acceptance of electronic identification means for both natural and legal persons; and
- provides guidelines for the State Electronic Certification System – Public Key Infrastructure (SECS).

According to this Decree-Law, and in line with the provisions of the eIDAS Regulation, affixing a qualified electronic signature to an electronic document holds the same legal weight as a handwritten signature on paper and establishes the presumption that:

- the person who affixed the qualified electronic signature is either its rightful holder or a representative authorised with adequate powers on behalf of the relevant legal person;
- the qualified electronic signature was affixed with the explicit intention of signing the electronic document; and
- the electronic document has remained unaltered since the qualified electronic signature was affixed.

Trusted List

In accordance with the eIDAS Regulation, each member state shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it

is responsible, together with information related to the qualified trust services provided by them.

This information is published in so-called trusted lists, and Commission Implementing Decision (EU) 2015/1505 defines the technical specifications of these lists.

The trusted list of Portugal comprises information concerning qualified trust service providers who are under the supervision of the National Security Cabinet of Portugal. This list also includes details regarding the qualified trusted services offered by these providers, in accordance with the relevant provisions outlined in the eIDAS Regulation.

The trusted list of Portugal includes the following currently active trust service providers:

- ACIN iCloud Solutions, Lda;
- AMA – *Agência para a Modernização Administrativa*, I.P.;
- CEGER – *Centro de Gestão da Rede Informática do Governo*;
- DigitalSign – *Certificadora Digital*;
- *Instituto dos Registos e do Notariado I.P.*
- MULTICERT – *Serviços de Certificação Eletrónica S.A.*; and
- *NOS Comuncações, S.A.*

The Portugal Digital Identity System

Portugal embarked on the development of its digital identity system in 2007, positioning itself as a pioneering nation in aggregating into a single card five different identification numbers and implementing digital certificates with its eID "Citizen Card". Since then, the Portuguese government has consistently invested in enhancing its eID scheme, introducing various secure and easy-to-use mechanisms.

In 2014, Portugal introduced the "Digital Mobile Key", a mobile solution that expanded its usage into the private sector. Subsequently, the eID schemes were broadened to include professional attributes (with the introduction of "SCAP", 2018). More recently, in 2019, Portugal launched the ID.gov app, a mobile application enabling citizens to securely store, access and share their personal document data at any time, with full legal validity.

9. Gaming Industry

9.1 Regulations

Regulations and Codes of Conduct

The gaming industry in Portugal is governed by a combination of general laws and sector-specific regulations, particularly where gaming intersects with gambling. The key legislative instruments include:

- The Gambling Law (Decree-Law No 66/2015): regulates online gambling activities, including games of chance, and establishes licensing requirements, taxation rules, and consumer protection measures;
- Consumer Protection Law (Law No 24/96): covers consumer rights, including transparency, advertising, and product liability, which may apply to digital gaming; and
- The GDPR and its National Implementation Regime: govern the collection, processing, and storage of player data by game developers and platforms.

While Portugal does not have a gaming-specific code of conduct, broader EU initiatives, such as the Pan-European Game Information (PEGI) system, apply to age ratings and content classification.

Key Legal Challenges

- Blurring lines between gaming and gambling: The inclusion of monetisation features such as loot boxes has drawn regulatory scrutiny to determine whether they constitute gambling under existing laws.
- Data protection and privacy: Adhering to the GDPR remains a significant challenge, especially for games with global user bases that rely on player data for analytics, personalisation, and monetisation.
- Consumer protection: Ensuring transparency in pricing, in-game purchases, and subscription models is crucial, particularly in safeguarding vulnerable users, including minors.

In-Game Purchases, Loot Boxes, and Gambling Elements

Portugal has not explicitly classified loot boxes as gambling. However, when these mechanisms resemble games of chance, they may fall within the scope of gambling regulations. The *Serviço de Regulação e Inspeção de Jogos* (SRIJ) monitors such practices to prevent unfair or exploitative practices.

Age Ratings and Content Restrictions

Portugal adheres to the PEGI rating system, requiring game developers to classify their games based on content such as violence, language, and gambling elements. Developers must:

- submit their games for PEGI classification before release; and
- display clear content warnings and age-appropriate labels on physical and digital copies.

Additionally, developers must ensure that game content does not violate Portuguese criminal or civil laws, including prohibitions against incitement to violence, hate speech, or other illegal activities.

9.2 Regulatory Bodies

Primary Regulatory Bodies

- *Serviço de Regulação e Inspeção de Jogos* (SRIJ): The SRIJ is the main regulatory body overseeing gambling activities, including both online and offline gaming with gambling elements. It is responsible for licensing, monitoring compliance, and enforcing gambling laws under the Gambling Law (Decree-Law No 66/2015). While primarily focused on games of chance, the SRIJ also monitors emerging concerns such as loot boxes and monetisation features in video games to assess potential gambling risks.
- *Autoridade Nacional de Comunicações* (ANACOM): ANACOM regulates digital platforms and telecommunications services relevant to gaming, particularly in areas such as internet services and network neutrality, which are crucial for online gaming operations.
- *Comissão Nacional de Proteção de Dados* (CNPD): The CNPD is responsible for ensuring compliance with the applicable data protection legislation. It oversees how gaming companies collect, process, and store user data, with a focus on games that feature online services, personalised content, and user tracking mechanisms.
- *Autoridade de Segurança Alimentar e Económica* (ASAE): ASAE enforces consumer protection laws, particularly regarding advertising transparency, pricing practices, and in-game purchases.

Recent Enforcement Actions

Unlicensed Gambling Platforms: The SRIJ has actively blocked access to numerous unlicensed online gambling websites. In recent years, several international gaming operators offering

unregulated gambling services have been fined or had their platforms blocked in Portugal.

9.3 Intellectual Property

Common IP Challenges for Game Developers

Game developers face several intellectual property challenges, particularly in an era of global digital distribution. Key issues include:

- Copyright infringement: The risk of piracy, unauthorised copying of game assets, and illegal distribution remains a significant concern. The rise of online gaming and streaming platforms has further exacerbated this issue.
- Licensing disputes: Developers frequently use licensed content, such as music, third-party characters, or proprietary game engines, which requires clear contractual agreements. Mismanagement of licensing rights can lead to legal disputes or liability.
- International IP protection: Ensuring IP protection across multiple jurisdictions is complex, particularly as games are distributed globally. Differences in copyright, trade mark, and software protection laws across countries can create enforcement challenges.

Legal Protections for IP in Virtual Environments

Portugal provides robust legal protections for game developers, covering both physical and virtual environments through various legal frameworks, as outlined below.

Copyright protection

- Under the Portuguese Code of Copyright and Related Rights, game developers automatically hold copyright over original creative elements, including graphics, storylines, soundtracks, and animations.
- Copyright protection applies regardless of the medium, ensuring coverage in both physical and digital environments.

Software protection

- Decree-Law No 252/94, implementing EU Directive 91/250/EEC, provides specific legal protection for computer programs. This law establishes that:
  (a) game software is treated as a literary work and is protected under copyright law;
  (b) developers hold exclusive rights over the reproduction, modification, and distribution of their software; and
  (c) users are only permitted limited exceptions, such as making back-up copies or engaging in reverse engineering for interoperability purposes.

Industrial property protection

- The Portuguese Industrial Property Code provides additional protections, including:
  (a) trade marks: protecting game titles, logos, and brand identifiers;
  (b) patents: applicable to unique game technologies, mechanics, and innovations; and
  (c) design registrations: covering game interfaces, character designs, and other visual elements.

Copyright in Digital and Virtual Assets

Game developers retain copyright over all original digital assets, such as character models, maps, animations, and in-game environments.

Protecting these assets requires:

- clear licensing agreements to establish ownership and usage rights; and

- Digital Rights Management (DRM) systems to prevent unauthorised access, copying, or distribution.

Special considerations apply to virtual economies, including in-game items and non-fungible tokens (NFTs). The legal status of these assets may vary depending on functionality and jurisdiction.

Trade Mark Laws for Virtual Goods and Services

- Trade marks safeguard brand names, logos, and other distinctive elements used in games and related services. In Portugal, trade marks can extend to virtual goods, such as branded in-game and digital assets.
- Developers must ensure that virtual goods replicating real-world brands (eg, virtual replicas of branded products) are properly licensed to avoid legal disputes.
- A growing trend involves registering trade marks specifically for use in virtual and metaverse environments to protect digital brand identity.

Implications of User-Generated Content (UGC)

User-generated content (UGC), such as mods, skins, maps, and custom game levels, raises significant IP challenges for game developers:

- Ownership disputes: Clear terms of service are essential to define whether UGC ownership rights belong to the developer or the user.
- IP infringement risks: Developers must actively monitor UGC to ensure it does not infringe on third-party copyrights, trade marks, or other legal protections. Failure to do so may result in liability for hosting infringing content.
- Monetisation and licensing: If UGC creators monetise their content (eg, through mod sales, in-game marketplaces, or content-sharing platforms), there must be:
  (a) defined licensing agreements to clarify usage rights and revenue-sharing models; and
  (b) clear policies on how UGC can be distributed, modified, or commercialised within the game's ecosystem.

10. Social Media

10.1 Laws and Regulations for Social Media

Main Laws and Regulations

Portugal does not have a specific national legal framework for social media. As an EU member state, Portugal is directly subject to EU legislation that impacts social media, either directly or indirectly.

Key applicable legal regimes include:

- Digital Services Act (DSA) – Regulation (EU) 2022/2065;
- General Data Protection Regulation (GDPR);
- Portuguese GDPR Implementation Law – Law No 58/2019;
- Privacy in Electronic Communications Law – Law No 41/2004;
- E-Commerce Law – Decree-Law No 7/2004, governing certain legal aspects of information society services, particularly electronic commerce, within the internal market;
- Portuguese Cybersecurity Law – Law No 46/2018; and
- Cybercrime Law – Law No 109/2009.

Additionally, the following legislation on contractual clauses, advertising, and consumer protection is also relevant:

- Standard Contractual Clauses Regime – Decree-Law No 446/85;
- Advertising Code – Decree-Law No 330/90 of 23 October;
- Consumer Protection Law – Law No 24/96;
- Unfair Commercial Practices Law – Decree-Law No 57/2008, regulating unfair practices in consumer transactions;
- Consumer Rights in Digital Transactions – Decree-Law No 84/2021, governing consumer rights in the purchase and sale of digital goods, content, and services;
- Distance and Off-Premises Contracts Law – Decree-Law No 24/2014; and
- Law on Individual Restrictive Trade Practices – Decree-Law No 166/2013.

Key Legal Challenges

Social media platforms operating in Portugal face important legal challenges, particularly in data protection, cybersecurity, and intellectual property enforcement.

Compliance with the GDPR and national data protection laws is essential, requiring platforms to ensure transparency in data processing, obtain valid user consent, and implement robust cybersecurity measures to protect user data from breaches.

Child protection and age verification remain critical concerns. Platforms must deploy effective systems to restrict access to age-inappropriate content and enforce stringent content moderation to prevent the dissemination of harmful material targeting minors. Additionally, the monetisation of user data raises legal and ethical issues regarding transparency, consent, and fairness under the GDPR, particularly in the context of targeted advertising and profiling.

Platforms must also combat hate speech and misinformation, particularly under the Digital Services Act (DSA), which mandates measures to prevent the spread of illegal content. Compliance with advertising regulations, including rules on influencer marketing and sponsored content, is crucial to mitigating legal and reputational risks.

Cross-border operations further complicate compliance, as platforms must adhere to both EU-wide and national regulations. To limit liability for user-generated content, platforms should implement proactive copyright protection measures, such as content filtering and notice-and-takedown systems.

10.2 Regulatory and Compliance Issues

The primary regulatory bodies overseeing social media in Portugal include:

- Portuguese Data Protection Authority (CNPD);
- Portuguese Electronic Communications Authority (ANACOM);
- National Cybersecurity Centre (CNCS);
- Food and Economic Safety Authority (ASAE);
- Directorate-General for Consumers (DGC); and
- Media Regulatory Authority (ERC).

These authorities have various enforcement powers, including the ability to:

- conduct inspections and audits to ensure compliance with applicable laws;
- impose fines for non-compliance; and
- mandate corrective measures, such as content removal, increased transparency in

advertising, and stricter age verification and privacy practices.

Additionally, consumer associations play a key role in monitoring and enforcement, particularly through class actions.

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