Chambers AND PARTNERS

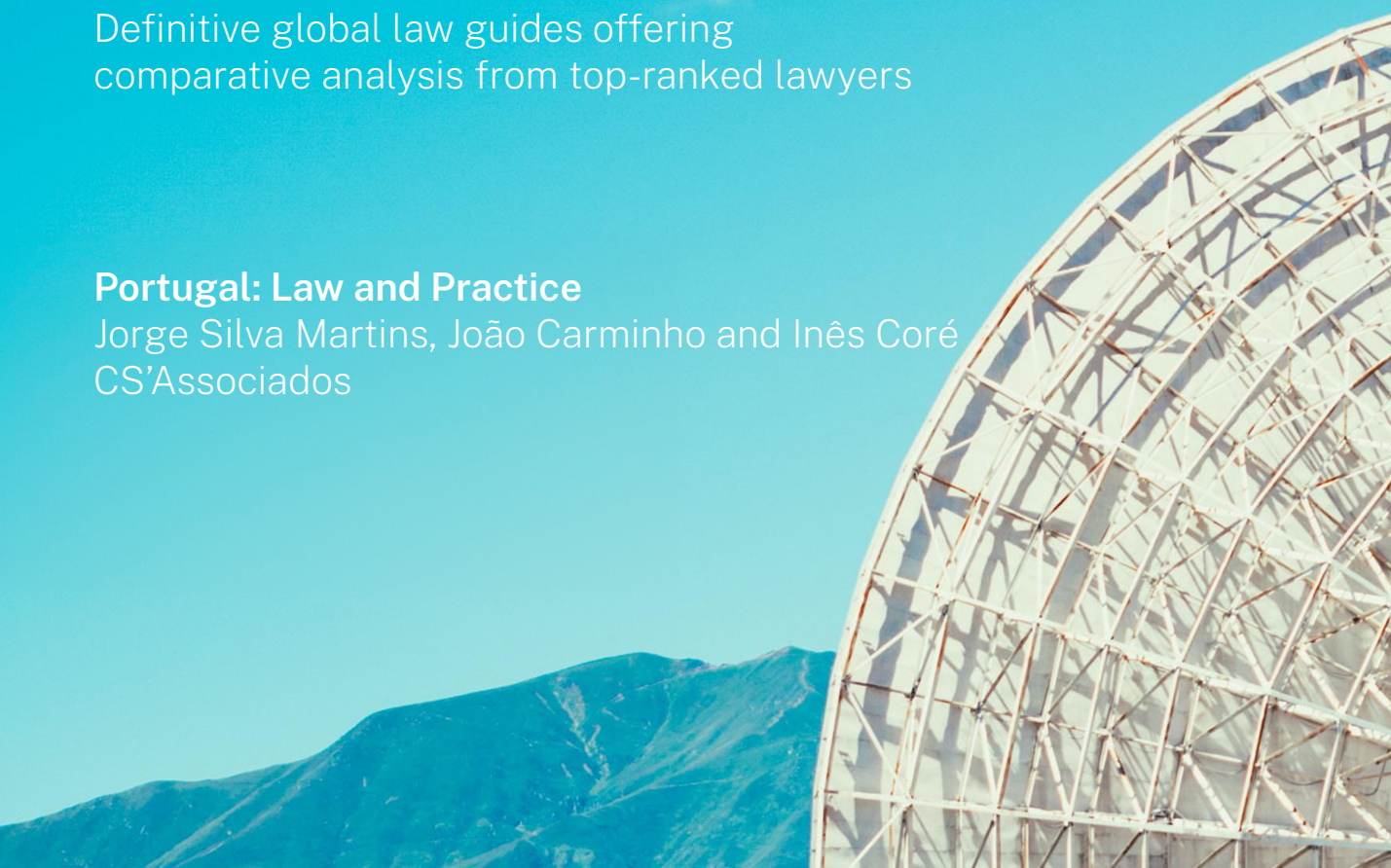
CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2024

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 based in Lisbon, serving national and international clients across the different sectors and industries. Through its technology, data and digital innovation practice area, the firm has been actively engaged with numerous companies within the highly dynamic TMT landscape, with a particular focus on electronic communications (including telco operators and towercos), e-commerce, internet law, media law, data protection, and intellectual property. Jorge Silva Martins leads the practice area, which also comprises three associates. Recent highlights include providing detailed advice for towercos in Portugal, conducting extensive regulatory assessments for product launches for one of the largest global technology companies, and offering legal and regulatory counsel to companies venturing into the realms of Web3 and the metaverse. Additionally, the firm has undertaken significant work involving the drafting and negotiation of agreements related to the development and implementation of software products for road infrastructures.

Authors

Jorge Silva Martins joined CS'Associados in January 2021 and leads the technology, data and digital innovation practice area. With nearly 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, e-commerce, internet law, media law, and intellectual property. Over the past few years, Jorge has expanded his expertise to encompass emerging technologies such as blockchain, the metaverse, and artificial intelligence. Additionally, he has authored several articles in the field of technology and is a regular speaker at industry and academic conferences.

João Carminho is a senior associate at CS'Associados in the technology, data and digital innovation practice area. He holds expertise in a range of sectors, such as electronic communications, e-commerce, privacy and data protection, and consumer law. João not only provides legal counsel to clients in these domains but also offers expert guidance in handling pre-litigation scenarios and facilitating dispute resolution before the relevant authorities. Through his comprehensive legal support, João actively contributes to clients' strategic decision-making within the dynamic landscape of technology, data and digital innovation.

Inês Coré is an associate at CS'Associados in the technology, data and digital innovation practice area. She offers legal assistance, focusing on matters related to data protection, intellectual property, and information technologies. Inês guides clients through the legal complexities associated with technology and innovation, providing continuous legal support to ensure compliance with ever-evolving regulations. As a member of the Portuguese Bar Association and the International Association for the Protection of Intellectual Property (AIPPI), Inês actively participates in a global network of professionals, which enables her to stay well-informed about international trends and best practices in the field of intellectual property.

CS'Associados

Avenida da Liberdade, No 249 – 8º
1250–143 Lisboa
Portugal

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

1. Metaverse

1.1 Laws and Regulation

Metaverses, Web3 (and Web 4.0)

Metaverses, also known as virtual worlds, are immersive technological environments that utilise 3D and extended reality (XR) to integrate physical and digital realms in real-time. They serve various purposes such as social interaction, transactions, and gaming. It is widely acknowledged that metaverses encompass three fundamental elements:

- persistence and real-time operation;
- immersive user experiences; and
- a generalised economic system.

Metaverses, or virtual worlds, are also part of a broader, long-term technological shift: the transition towards Web3 and Web 4.0 (the third and fourth iterations of the World Wide Web). These advancements aim to seamlessly merge physical and digital domains, fostering more intuitive and immersive experiences. This convergence is anticipated through the evolution of diverse technologies, including artificial intelligence (AI), the internet of things (IoT), secure blockchain transactions, as well as the continuous improvement in infrastructure connectivity.

State of Play

Similar to the situation in the vast majority of countries, Portugal currently lacks specific domestic legislation governing the metaverse. However, as a member state of the EU, Portugal aligns with the European approach to the metaverse, which is worth highlighting.

While previous documents, such as the European Commission Communication dated 16 March 2023, and the European Council conclusions dated 23 March 2023, have made references to Web 4.0 (as a digital tool to enhance the EU's long-term competitiveness), it is in the Communication dated 11 July 2023, that the European Commission (EC) outlines its strategy and proposed actions regarding Web 4.0 and virtual worlds, aimed at guiding the forthcoming technological transition while ensuring an open, secure, trustworthy, fair and inclusive digital environment for EU citizens, businesses and public administrations.

To this end, the EU has already in place a robust, future-oriented legal framework that addresses various aspects of virtual worlds development, including:

- With regard to the protection of intellectual property rights (including industrial rights), the following legislative frameworks generally apply:
  - (a) Directive on Copyright in the Digital Single Market (Directive (EU) 2019/790, transposed into Portuguese law by Decree-Law No 47/2023);
  - (b) Regulation on the EU Trademark (Regulation (EU) 2017/1001); and
  - (c) Directive on the Protection of Trade Secrets (Directive (EU) 2016/943, transposed into Portuguese law by Decree-Law No 11/2018).
- With regard to the protection and enforcement of rights of EU citizens and companies operating in the metaverse, the following regimes generally apply:
  - (a) Digital Services Act or DSA (Regulation (EU) 2022/2065);
  - (b) Digital Markets Act or DMA (Regulation (EU) 2022/1925);
  - (c) Data Governance Act (Regulation (EU) 2022/868);
  - (d) Data Act (Regulation (EU) 2023/2854);
  - (e) AI Act (pending EU-level approval);

(f) GDPR (Regulation (EU) 2016/679);
(g) General Product Safety Regulation (Regulation (EU) 2023/988);
(h) Markets in Crypto-Assets (MiCA) Regulation (EU) 2023/1114);
(i) Unfair Commercial Practices Directive (Directive (EU) 2005/29, transposed into Portuguese Law by Decree-Law No 57/2008);
(j) Accessibility Act (Directive (EU) 2019/882, transposed into Portuguese Law by Decree-Law No 82/2022); and
(k) Web Accessibility Directive (Directive (EU) 2016/2102, transposed into Portuguese law by Decree-Law No 83/2018).

Additionally, standardisation will also play a pivotal role in achieving trustworthy, secure and interoperable metaverses within the EU. In that regard, the EC has closely engaged with relevant industry stakeholders to develop standards that ensure openness and interoperability across all layers of the metaverse.

Key Legal Challenges

Although the legal landscape on metaverse is still evolving, there are several legal challenges to consider, namely with regard to the following.

- Intellectual property – safeguarding virtual assets within the metaverse (eg, virtual real estate, digital goods, and in-game currencies); addressing copyright concerns related to user-generated content within the metaverse; and determining platform operator's liability for copyright infringement.
- Data protection – addressing privacy concerns related to user data generated within the metaverse and the processing of special categories of data (eg, biometric data); and clarifying ownership and control of personal data in virtual environments.
- Cybersecurity – ensuring secure identity verification and authentication mechanisms to prevent unauthorised access to virtual spaces; protecting user accounts; and securing financial transactions within the metaverse.

2. Digital Economy

2.1 Key Challenges

Introduction

The digital economy is the economic activity stemming from billions of daily online interactions among individuals, businesses, devices, data and processes. At its core, the digital economy thrives on hyperconnectivity, characterised by the increasing interconnection of people, organisations and machines facilitated by the internet, mobile technology, and the IoT.

A growing variety of mobile devices, such as smartphones, tablets, smartwatches and wearables, empower billions worldwide to participate in the digital economy, accessing goods and services on a global scale, at any time and from any location. While this connectivity offers numerous benefits, it also requires intense regulation.

Advantages of the Digital Economy

The digital economy is positioned to wield even greater influence in the future, propelled by advancements in technologies such as the IoT, AI, virtual reality, blockchain, self-driving cars and other ground-breaking developments. Among its many advantages are:

- information accessibility – consumers have access to a wealth of information to inform their purchasing decisions;
- proximity – direct customer service channels enable customers to resolve queries and

issues with a manufacturer or service provider more quickly;
- global reach – businesses can expand their market presence as goods and services become accessible worldwide; and
- security – digital technologies, including robust authentication for online transactions, bolster security measures.

European Union

The digital economy is playing an ever-increasing role in our lives, revolutionising the way we conduct business, communicate and access information.

As this transformation accelerates, effective regulation becomes paramount to ensure fair competition, protect citizens' rights, and address emerging challenges.

Governments worldwide are grappling with the task of formulating comprehensive regulatory frameworks that set a balance between fostering innovation and mitigating potential risks. Key areas of focus include data privacy, cybersecurity, antitrust, consumer protection and intellectual property rights. Policymakers are challenged to keep pace with the rapid evolution of technology, adapt regulations to address novel issues, such as AI and blockchain, and foster international cooperation to create a harmonised approach to the global digital economy.

To achieve this equilibrium, the EU has implemented a comprehensive framework of digital legislation, primarily through the Digital Agenda and the Digital Single Market (DSM) initiatives. Recent legislative efforts, such as the Digital Markets Act (DMA), the Digital Services Act (DSA), the Data Act, the (forthcoming) Artificial Intelligence Act (AI Act), the Data Governance Act (DGA), the (forthcoming) European Health Data Space (EHDS), and the NIS2 Directive (imposing stricter cybersecurity obligations on entities operating critical infrastructures and essential services), along with the upcoming eIDAS 2.0, emphasise the EU's commitment to digital governance.

As a member of the EU, Portugal aligns its national policies with the Union's overarching digital strategies.

Portugal

On 5 March 2020, the Presidency of the Council of Ministers approved Portugal's Action Plan for Digital Transition, outlining the government's vision in this regard. This Plan revolves around three primary pillars:

- Pillar I – Capacity building and digital inclusion;
- Pillar II – Businesses' digital transformation; and
- Pillar III – Public services' digitalisation.

In this context, reference should also be made to the following legislation passed in recent years:

- Law No 46/2018, which establishes the legal framework for cyberspace security, implementing Directive (EU) 2016/1148, concerning measures for a high common level of security of network and information systems across the EU;
- Law No 58/2019, implementing the General Data Protection Regulation;
- Decree-Law No 12/2021, implementing Regulation (EU) 910/2014 on 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, which regulates the legal framework for cyberspace security and defines cybersecurity certification obligations implementing Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification;
- 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, both of 20 May 2019; and
- Law No 16/2022, which approves the new electronic communications law.

Main Challenges

Despite of the benefits resulting from the digital economy, several challenges persist, including the need for further investment in digital infrastructure, addressing the digital skills gap, and ensuring equitable distribution of its benefits across regions.

Portugal's policymakers are actively shaping a regulatory environment to support the digital economy's growth while confronting emerging issues. However, challenges remain, such as the following.

- Data utilisation – access to big data can create disparities in competitiveness.
- Platform practices – concerns exist regarding competition restrictions and opaque data processing models.
- Regulatory adaptation – in sectors regulated by rapid technological innovation, adapting regulations to keep up with these changes can be a complex undertaking.
- Stakeholder collaboration – the proper implementation of EU regulations often requires the collaboration of various sectors, including governments, companies, non-governmental organisations and other stakeholders. Co-ordination and support from all these entities can take time, especially when there are different interests and perspectives that need to be reconciled.
- Implementation hurdles – complex regulations and resource constraints may impede timely implementation. Also, some regulations may require significant changes to existing systems and infrastructure, both in the public and private sectors. This can require substantial investments in terms of time and financial resources.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Introduction

Cloud computing involves the delivery of computing services, such as storage, processing power and applications over the internet. It allows businesses to access and utilise shared resources, without the need for on-site infrastructure, offering flexibility and cost-effectiveness. In contrast, edge computing involves processing data closer to the source of data generation, reducing latency and enhancing real-time capabilities. It often involves decentralised infrastructure, enabling data processing at the edge of the network, closer to end-users or devices.

These technologies have revolutionised the way businesses operate, offering unprecedented scalability, efficiency and accessibility. However,

in addition to these benefits, they also present risks that need to be addressed, in particular in terms of data protection, privacy and security.

EU

At European level, the regulation of these technologies is essentially ensured by the GDPR, which lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data, with special emphasis on:

- security of the processing;
- processing by processors; and
- data transfers to third countries.

In accordance with the GDPR:

- Controllers and processors must implement appropriate technical and organisational measures, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to ensure a level of security appropriate to the risk.
- When processing is conducted on behalf of a controller, the controller must engage processors who offer adequate guarantees to meet the Regulation's requirements and safeguard the rights of data subjects. This processing shall be governed by a binding contract or other legal act under Union or member state law, specifying the processing's subject-matter, duration, nature, purpose, types of personal data, and categories of data subjects. This contract must also contain the minimum content provided for in Article 28(3) of the GDPR.
- Transfers of personal data to third countries of international organisations must adhere to Chapter V of the GDPR. Key conditions include (i) the existence of an adequacy decision by the European Commission; (ii) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2) of the GDPR; and (iii) binding corporate rules in accordance with Article 47 of the GDPR.

It should also be noted that:

- industries dealing with significant amounts of personal data or sensitive data (eg, healthcare, banking and finance, telecommunications and insurance) face stricter processing security standards;
- providers of these technologies are typically classified as processors under the GDPR; and
- additional safeguards may be required for transferring personal data to the US.

Portugal

In Portugal, alongside EU Regulations, the following legislation must also be taken into account:

- Law No 46/2018, which establishes the legal framework for cyberspace security, transposing Directive (EU) 2016/1148, concerning measures for a high common level of security of network and information systems across the Union;
- Law No 58/2019, which ensures the implementation, in the national legal system, of the GDPR; and
- Portuguese Data Protection Authority (CNPD) Guideline No 2023/1, on organisational and security measures applicable to the processing of personal data.

As cloud and edge computing continue to evolve, the aforementioned legislation should be adapted and updated to address emerging challenges and promote innovation, while maintaining a balance between technological advancement and the rights, freedoms and guarantees of data subjects.

4. Artificial Intelligence

4.1 Liability, Data Protection, IP and Fundamental Rights

Legal Concept of AI

An AI system is defined by law (as per the Artificial Intelligence Act) as a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments.

AI systems are thus a "family" of technologies with virtually limitless applications, offering substantial benefits to individuals, companies and society as a whole.

Nonetheless, while many AI systems are harmless and contribute to solve many societal challenges, others might pose risks to individuals and jeopardise their health, safety or fundamental rights.

Portugal

For the time being, there is no specific law on AI in Portugal. However, there are references to the use of AI (especially with regard to the limits of its use) in several national regimes, namely:

- Portuguese Charter on Human Rights in the Digital Age (Law No 27/2021); and
- Portuguese Labour Code (Law No 7/2009).

The respect for fundamental rights, both with regard to the design and use of AI and robots is enshrined in Article 9 of the Portuguese Charter on Human Rights in the Digital Age, which foresees that AI should comply with several ethical principles, including transparency, accountability and non-discrimination.

Similarly, the Portuguese Labour Code sets limits to the use of AI whenever it results in decision-making that jeopardises the exercise of employee's rights provided for by law (such as the right to equal opportunities in the access to the labour market). On the other hand, it establishes information duties with regard to the criteria on which AI algorithms are based for the decision-making process.

Moreover, the Portuguese government has also published several legislative initiatives and strategies which make reference to AI technologies and their development and impact within the Portuguese society.

Anyhow, a comprehensive AI legal framework is mainly being shaped at an EU level, which is understood to be in the forefront of AI regulation.

EU

As Portugal is a member state of the EU, the regulation proposal on AI (Artificial Intelligence Act), expected to be approved next April, will soon be part of the Portuguese legal system.

The Artificial Intelligence Act, proposed by the European Commission (EC) on 21 April 2021 (regarded as the world's first comprehensive AI law) aims primarily to establish a robust internal

market for AI systems within the EU. Its objectives are two-fold: to ensure that the EU remains at the cutting edge of technological advancement, and to safeguard the rights of EU citizens. The Artificial Intelligence Act will thus establish different obligations for providers and users depending on the level of risk posed by the AI system (minimal risk, high risk, unacceptable risk, and specific transparency risk), and will apply to both public and private actors inside and outside the EU, provided that the AI system is placed on the EU market or its use affects people located in the EU.

Moreover, AI will also be regulated under the following legal frameworks within the EU:

- AI Liability Directive; and
- Product Liability Directive.

Both the AI Liability Directive and the Product Liability Directive (which have not yet been adopted) were proposed by the EC on 28 September 2022, and aim to adapt liability rules to the digital age amongst the member states.

On the one hand, the Product Liability Directive intends to update the existing rules on non-fault (strict) civil liability of manufacturers for defective products (including AI systems which are also regarded as products), while the AI Liability Directive targets harmonisation of national non-contractual fault-based civil liability rules for AI in specific. The idea is to facilitate compensation to victims of unsafe products and AI-related damage, respectively.

In short, AI Liability Directive simplifies the legal procedure for victims seeking compensation by facilitating proof that someone's fault led to damage under the following legal mechanisms.

- Presumption of causality – where a relevant fault has been established and a causal link to the AI performance seems likely there is a presumption of a causal link between such non-compliance and the output produced by the AI system.
- Evidence disclosure – where damage is caused by high-risk AI systems, victims have a right of access to evidence from providers or users pursuant to the Artificial Intelligence Act.

AI Liability Directive will thus apply to claims against any person which, due to wrongful behaviour, influenced AI systems in causing damage (any type of damage covered under national law) to either natural or legal persons (ie, individuals or businesses), whereas the Product Liability Directive will apply to claims against manufacturers of defective products for the compensation of personal injury, damage to property or data loss caused by unsafe products, and it is limited to claims made by natural persons (ie, individuals).

Once adopted, all these regimes will certainly bring significant changes to national liability and consumer protection rules.

Moreover, as AI systems process vast quantities of data, the following legal frameworks may have implications for data sharing and data usage under this context:

- General Data Protection Regulation or GDPR (Regulation (EU) 2016/679);
- Data Act (Regulation (EU) 2023/2854);
- Data Governance Act (Regulation (EU) 2022/868); and
- Digital Services Act or DSA (Regulation (EU) 2022/2065).

Specifically with regards to data protection, key requirements for the development of AI technologies will have to be taken into consideration, such as data minimisation (Article 5(1)(c) of the GDPR) or privacy by design and by default (Article 25 of the GDPR).

Codes of Conduct

Furthermore, concerning codes of conduct, the European AI Alliance has devised an AI Impact Assessment (AIIA) which, in essence, is a practical tool that aims to help organisations to design, employ and audit AI.

The starting point of the AIIA is the Code of Conduct for AI, which forms the basis of the AIIA framework. The Artificial Intelligence Code of Conduct thus consists of two parts:

- common European ethical and constitutional values (ie, 1791 liberty, equality, fraternity), legal principles (eg, fairness, proportionality, rule of law) and democratic preconditions; and
- practical rules and codes of conduct for, inter alia, AI applications, the training data corpora, inference systems, deep learning algorithms, neural networks and autonomous systems.

5. Internet of Things

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

IoT at a Glance

The internet of things (IoT) has been defined in a variety of ways, but it is commonly understood as referring to a global distributed network of physical objects which are capable of interacting with their environment and communicating with each other (including other machines or computers), and are thus regarded as "smart objects".

The value of these objects (which can either be household appliances and small wearables or even cars and industrial robots) lies in the large amount of data they collect and process in order to communicate with each other. As IoT results in the merging between both the physical and digital worlds, it enables the creation of "smart environments", giving rise to specific realities, including "smart homes" (ie, IoT applied to the management and control of buildings, such as lighting or heating) or "smart cities" (ie, IoT applied to the management and control of city infrastructures, such as traffic or public transport).

Portugal

For the time being, Portugal does not have specific laws pertaining to IoT. However, the Portuguese government has introduced legislative initiatives and strategies that address IoT's development and its impact on Portuguese society.

EU

As Portugal is a member state of the EU, IoT regulation at a EU level is worth highlighting. In that regard, the EU is currently actively cooperating with the industry, market players and academia to support research, innovation and development of IoT technologies.

A number of supporting policy actions have thus been adopted by the EC to enhance development of IoT, particularly through funding research and large-scale pilot projects. However, there are no EU regulatory frameworks specifically targeting IoT technologies, apart from the references made below.

Data Protection and IoT

As IoT largely relies on the processing of data to enable Machine-to-Machine Communications, its regulation will necessarily fall under the applicable data protection legal framework, namely:

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

The development and usage of IoT will thus have to respect the fundamental right to data protection enshrined in Article 8 of the Charter of Fundamental Rights of the European Union.

IoT technologies may indeed pose threats to personal data protection, since "smart objects" (such as wearables) might often collect personal data, including, special categories of personal data revealing, for instance, data concerning health (Article 9 of the GDPR). It is precisely through the collection of the said data, as well as its combination with other sets of data that it is possible to establish patterns and further enhance the "smart object" performance for the benefit of the user. On the other hand, security risks might give rise to a "personal data breach" (Article 4(12) of the GDPR) and compromise the integrity of the personal data through unlawful access.

The Data Act (which entered into force on 11 January 2024) regulates data generated by a user's product connected to a publicly available electronic communications network, and aims at harmonising rules on the fair access to and use of such data. In other words, it clarifies who can create value from data and under which conditions. This is indeed relevant for IoT technologies since "smart products" rely immensely on data gathered from its users.

The Data Act will become applicable from 12 September 2025 and creates measures to, namely:

- give access to businesses and consumers of IoT technologies to the data generated by these devices;
- protect businesses from unfair contractual terms that hinder fair data sharing;
- allow public sector bodies to access and use data held by the private sector that is necessary for the pursuit of public interest purposes; and
- allow customers to seamlessly switch between different cloud providers of data-processing services.

The aforementioned measures complement the Data Governance Act (that became applicable from 24 September 2023), which together with the Data Act embody the EU Strategy for Data.

The Data Governance Act focus on data-sharing, regulating processes and structures to facilitate such exchange, namely through the following measures:

- facilitate the reuse of public sector data that cannot be made available as open data;
- ensure that data intermediaries function as trustworthy organisers of data sharing or pooling within the EU data spaces;
- make it easier for citizens and businesses to make their data available for the benefit of society; and
- facilitate data sharing, in order to enable data use across sectors and borders.

Overall, both the Data Act and the Data Governance Act complement existing rights on personal data protection. This applies in particular to the right to data portability (Article 20 of the GDPR) that allows data subjects to move their data between controllers who offer competing services.

Communications Secrecy

Communications secrecy within the context of IoT technologies falls under broader regulations mainly related to data protection, cybersecurity and consumer rights.

Apart from GDPR applicability, which was already addressed, the ePrivacy Directive (Directive 2002/58/EC) regulates the protection of personal data and privacy in electronic communications. While the ePrivacy Directive is currently in force, a new ePrivacy Regulation is under discussion and is expected to update and strengthen privacy rules for electronic communications, including IoT devices.

On the other hand, NIS2 Directive (Directive (EU) 2022/2555) which entered into force on 16 January 2023 replacing its predecessor NIS Directive, is considered the EU-wide legislation on cybersecurity and although it does not specifically target IoT, it has implications for the overall cybersecurity of systems, which indirectly influences communication secrecy within IoT deployments.

Moreover, considering the security risks that products with digital elements may entail (including, IoT technologies), the EC adopted a proposal for a regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).

Codes of Conduct

With regard to codes of conduct and standards, the European Telecommunications Standards Institute (ETSI) has developed standards and technical specifications pertaining to IoT security and privacy. These standards encompass requirements, architecture, Application Programming Interface (API) specifications, security solutions and interoperability for Machine-to-Machine (M2M) communications. Additionally, the International Organization for Standardization (ISO) has published ISO/IEC 27400:2022, providing guidelines on risks, principles and controls for the security and privacy of IoT solutions.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Provision of Audio–Visual Media Services in Portugal

Audio–visual media services (AVMS) in Portugal are mainly regulated under the following legislation:

- Decree-Law No 46/2023 (implementing Directive (UE) 2019/789 on Copyright and Related Rights applicable to certain Online Transmissions of Broadcasting Organisations and Retransmissions of Television and Radio Programmes);
- Decree-Law No 47/2023 (implementing Directive (UE) 2019/790 on Copyright and Related Rights in the Digital Single Market or DSM Directive);
- Decree-Law No 82/2022 (implementing Directive (UE) 2019/882 on Accessibility Requirements for Products and Services);

- Law No 74/2020 (implementing Directive (UE) 2018/1808 or Audiovisual Media Services Directive);
- Law 54/2010 (Radio Act);
- Law No 27/2007 (TV and On-demand Audio–Visual Services or AVMS Law implementing Directive (EU) 2010/13 on Audiovisual Media Services); and
- Decree-Law No 63/85 (Copyright and Related Rights Code).

As pursuant to the applicable law, 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 by video-sharing platform providers.

The aforementioned legislation stipulates several requirements that must be met by AVMS providers. Namely, all audiovisual media services are required to adhere to the following obligations:

- identification of media service providers;
- prohibition of incitement to hatred;
- accessibility for people with disabilities;
- qualitative requirements for commercial communications;
- sponsoring; and
- product placement.

More stringent rules in the areas of advertising and protection of minors are foreseen for television broadcasts, due to their significant societal impact, as elaborated below.

In accordance with the Portuguese AVMS Law, AVMS are thus obliged to respect fundamental rights within their programming content, and may not (i) provoke or incite any violence or hatred towards a particular group of people (eg, minorities); and (ii) provoke or incite the commitment 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 can only be made available during times when minors are unlikely to view them (ie, between 10pm and 6am), and must be identified by the presence of a visual symbol throughout its duration.

The same applies to on-demand audio–visual service providers, who are also obliged to identify such content through a visual symbol. Furthermore, they are required to implement technical functionalities that enable individuals responsible for parental oversight to block minors' access to such content.

Nonetheless, on-demand audio–visual media services are different from television broadcasting (namely, with regard to the choice and control of the user or the impact they have within society) which has justified the imposition of lighter regulation.

With regard to advertising, television commercials and teleshopping aired from 6am to 6pm, as well as from 6pm to midnight, must not surpass 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

Regarding video-sharing platform services, some of the aforementioned requirements will also be applicable. The obligations primarily focus on protecting minors and the general public from hate speech, and well as prohibiting the incitement of violence and other forms of hateful content, including criminal and child pornographic material. Therefore, video-sharing platforms are mandated to moderate user-generated content to a certain extent to ensure compliance with these obligations.

Moreover, following the entry into force of the Regulation (EU) 2022/2065 (Digital Services Act or DSA), video-sharing platforms are also required to comply with several measures aimed at combating illegal content online.

Authorisation Procedure

Pursuant to Article 13 of the AVMS Law, television activities are subject to licensing through a public tender, initiated by the government's decision, when utilising terrestrial radio spectrum for broadcasting. The licensed activities encompass (i) organising unconditional access television programme services, and (ii) selecting and aggregating television programme services with conditional access or non-conditional access with subscription.

When television activities involve organising programme services that (i) do not utilise the terrestrial radio spectrum designated for broadcasting, and (ii) are intended to be included in the offerings of a distribution operator previously licensed for television activities, an authorisation is required upon the request of interested parties. Moreover, providers of on-demand audio–visual services are obliged to electronically notify ERC of the commencement and conclusion of each service's activity. *Entidade Reguladora para a Comunicação Social* (ERC) – Portuguese Regulatory Authority for the Media – holds the responsibility for granting, renewing, amending, or revoking licences and authorisations for television activities.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Regulatory Framework

In Portugal, the regulation of electronic communications networks and services is governed by numerous legislative acts and regulations, including:

- Electronic Communications Law (Law No 16/2022);
- Communications Infrastructures Law (Decree-Law No 123/2009);
- Privacy in electronic communications Law (Law No 41/2004); and
- Portuguese Cybersecurity Law (Law No 46/2018).

ANACOM serves as the sector-specific regulatory authority, as outlined in its Statutes (Decree-Law No 39/2015).

Moreover, the Portuguese Competition Authority is responsible for monitoring post-market conditions in the electronic communications sector. Oversight of social media platforms may fall within the jurisdiction of the Portuguese Regulatory Authority for the Media (ERC – *Entidade Reguladora para a Comunicação Social*), especially when these platforms operate as broadcasting outlets or are supervised by ANACOM regarding the provision of information society services. Regarding privacy matters, social media platforms fall under the supervision of the

Portuguese Data Protection Authority (CNPD), as stipulated in Law No 58/2019.

The Portuguese Electronic Communications Law

Following a protracted period marked by stagnation and procedural delays, the European Electronic Communications Code (EECC) was finally transposed into national law in Portugal.

Published in the official gazette, Law No 16/2022, marks the enactment of the new Electronic Communications Law (referred to as the "New ECL"). This law heralds a modernised, forward-looking regulatory framework that requires familiarity from all stakeholders, including operators and end-users.

The New ECL represents a comprehensive, intricate regime that closely mirrors the objectives and verbiage of the EECC. Notably, deviations from the EECC's text are most apparent in the realm of end-users' rights, which is not unexpected, given the focal point these rights held in parliamentary deliberations throughout the domestic legislative process.

Comparatively, the New ECL introduces noteworthy alterations from the existing regulatory framework, including the following.

- Broader definition of Electronic Communications Services – the New ECL broadens the definition of electronic communications services to include OTT services, which are services delivered over the internet, such as messaging apps and VoIP calling. This expansion reflects the evolving landscape of communication technologies and ensures that regulatory frameworks remain updated and comprehensive.
- Lighter regulations for OTT Services – while OTT services fall within the scope of the New ECL, they are subject to a more lenient regulatory regime compared to traditional electronic communication services. For instance, they may not require general authorisation for provision (depending on their nature) and are exempt from certain general conditions applicable to traditional services.
- Spectrum management powers – ANACOM gains enhanced powers in managing radio spectrum. This includes promoting spectrum sharing among operators to maximise efficiency and ensuring fair competition. ANACOM is also empowered to adjust the duration of frequency rights to prevent distortions in the market.
- Market power obligations – undertakings with significant market power face reinforced obligations, including providing access to infrastructure and commitments to invest in high-capacity networks. These measures aim to foster competition and encourage investment in critical telecommunications infrastructure.
- Consumer protections – the New ECL strengthens consumer protections in various ways. It mandates transparency regarding setup costs and service quality, provides consumers with tools to compare prices and conditions across different services, and offers safeguards in cases of service unavailability or non-compliance with service level agreements (SLAs). Additionally, it regulates minimum contractual commitment periods, ensuring fairness and flexibility for consumers.
- Social regulation challenges – despite advancements in regulatory frameworks, challenges remain in social regulation, particularly concerning universal service provisions. The reliance on the internet social tariff rather than the New ECL's provisions raises

questions about the effectiveness of achieving social objectives in the digital age.
- Implementation and enforcement – contractual commitments under the new law apply to both existing and future contracts, ensuring continuity and consistency in consumer rights and obligations.

These changes reflect Portugal's efforts to modernise its telecommunications regulatory framework, aligning with European standards, while addressing evolving technologies and consumer needs.

Requirements

The aforementioned legislation outlines the applicable general authorisation requirements in this regard. According to these requirements, individuals or companies planning to offer publicly accessible or private electronic communications networks and services are obligated to inform ANACOM before introducing these services in the market.

The notification submitted to ANACOM should include a concise written description of the network or service and the anticipated launch date for market offerings. More details on the notification process to ANACOM are further specified under the applicable regulation, which addresses the registration of entities providing electronic communications networks and services, as well as outlines information responsibilities to fall upon entities governed by the regulation.

Within the framework of general authorisation rules, any entity engaged in offering electronic communications networks and/or services has the permission to deploy telecommunications infrastructure. However, specific licences, such as administrative authorisations mandated by municipalities may still be necessary.

Therefore, and in accordance with the general authorisation rules, companies are required to provide the following information.

- Comprehensive company identification, encompassing the company's website linked to the provision of publicly available electronic communications networks and services.
- Communication and notification contacts, inclusive of a mandatory email address.
- A concise overview of the network or service they intend to deliver, specifying the network or service type, target market (wholesale or retail), support network for the service, information on the network's characteristics and purpose, the necessity for numbering or frequency resources, and a specification of said resources. Additionally, a general description of the service offer is required.
- The anticipated commencement date for operations.

A noteworthy change brought about by the New ECL pertains to the utilisation of harmonised spectrum for accessing public electronic communications networks through radio, specifically via local networks (such as WiFi networks deployed using LANs in end-users' premises). This particular usage is exclusively governed by the general authorisation framework.

The New ECL explicitly states that the provision of number-independent interpersonal communications services and local networks via radio, when not constituting an economic activity or carried out as an ancillary function to an economic activity or public service not reliant on the conveyance of signals over that network, is exempt from the general authorisation framework, regardless of the entity – be it a company, public authority, or end-user.

Individual licences are granted for the utilisation of numbering and frequency resources.

The provision of electronic communications services for self-use is categorised as non-publicly available.

Main Challenges

The challenges within Portugal's electronic communications regulatory framework primarily centre on securing fair access to communication services, bridging the digital divide and adapting to the swift evolution of technology and business models. There is a pressing need to effectively implement universal service provisions, especially in underserved communities, while grappling with complexities such as digital inclusion, privacy concerns, and cybersecurity threats. Balancing innovation and investment with regulatory oversight, ensuring compliance with evolving EU legislation and fostering collaboration between stakeholders are crucial for maintaining a robust and responsive regulatory framework in an increasingly digital landscape.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Introduction

A technology agreement can be defined as an agreement focusing on technological products and/or services, or those incorporating a technological component. This can apply to various types of agreements, including:

- Software licence agreements.
- Technology transfer agreements.
- Service level agreements.
- Research and development agreements.
- Non-disclosure agreements.
- Joint-venture agreements.
- Outsourcing agreements.
- Hardware purchase agreements.

These agreements generally contain clauses on the rights and obligations of both parties, price, terms of invoicing and payment, intellectual property rights, confidentiality, processing of personal data, duration, termination, liability, assignment of the contractual position and subcontracting, audits, communications, applicable law and jurisdiction, among others.

Challenges

In addition to the challenges associated with drafting clauses on the aforementioned topics – which are common to contracts of any nature – these agreements pose specific challenges, linked to the swift evolution of technology and related legislation. This evolution can result in outdated terms and conditions that may not adequately address emerging technologies and associated risks. Some of these challenges include the following.

- Data privacy and security concerns – with the heightened emphasis on data privacy and security, technology agreements must address these concerns. This is especially crucial in regulated sectors and industries handling significant amounts of personal data (eg, healthcare, banking and finance, telecommunications and insurance), where stringent security standards apply.
- Global operations and jurisdictional complexities – technology agreements involving parties from different jurisdictions often encounter challenges due to legal and regulatory disparities. Determining the applicable laws and jurisdictions for dispute resolution can be intricate and requires careful consideration.

- Performance and service level challenges – defining and measuring performance metrics in service level agreements can be challenging. Ensuring that technology services adhere to agreed-upon standards may require ongoing monitoring and adjustment to maintain satisfactory levels of performance.
- Contractual interpretation – ambiguities in language within technology agreements can lead to misunderstandings and disputes. It is imperative to provide clear definitions, specifications, and obligations to minimise the risk of misinterpretation and ensure smooth contractual execution.
- Cybersecurity vulnerabilities – as technological interconnectedness grows, so does the likelihood of cybersecurity threats. Technology agreements must incorporate robust cybersecurity measures and response protocols to mitigate potential risks.

Addressing these challenges requires thorough due diligence, seeking legal counsel, and consistently reviewing and updating technology agreements. This ensures their ongoing relevance and effectiveness in the ever evolving technology landscape.

Moreover, integrating flexibility into agreements to accommodate changes and unforeseen circumstances can facilitate in mitigating some of these challenges.

Portugal

In Portugal, there is no specific regulation applying to technology agreements. Consequently, these agreements are typically governed by overarching legal principles and rules of private law, in particular, the Civil Code and Commercial Code.

In addition to these two fundamental regimes, there are also some specific frameworks that deserve to be highlighted 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. This Directive was repealed by Directive 2009/24/EC, of the European Parliament and of the Council, of 23 April 2009, addressing the same subject.
- 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.
- Decree-Law No 446/85, which approves the Standard Contractual Clauses Regime.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

Introduction

According to the Regulation (EU) No 910/2014, of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market ("eIDAS Regulation"):

- "Electronic signature" means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

- "Advanced electronic signature" means an electronic signature which meets the following requirements:
  (a) it is uniquely linked to the signatory;
  (b) it is capable of identifying the signatory;
  (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
  (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
- "Qualified electronic signature" means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.
- "Trust service" means an electronic service normally provided for remuneration which consists of:
  (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services;
  (b) the creation, verification and validation of certificates for website authentication; or
  (c) the preservation of electronic signatures, seals or certificates related to those services.
- "Qualified trust service" means a trust service that meets the applicable requirements laid down in this Regulation.

In accordance with this Regulation:

- an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures;
- a qualified electronic signature shall have the equivalent legal effect of a handwritten signature; and
- a qualified electronic signature based on a qualified certificate issued in one member state shall be recognised as a qualified electronic signature in all other member states.

Importance and Advantages of Trust Services and Electronic Signatures

Trust services and electronic signatures offer essential advantages for companies in the digital era. One key benefit is the significant time and cost savings achieved by streamlining document workflows and eliminating the need for physical signatures. Electronic signatures expedite approval cycles, reduce administrative overheads and enhance overall operational efficiency.

Security emerges as another critical factor. Trust services provide advanced security measures such as encryption and authentication, safeguarding the integrity and confidentiality of digital transactions. Supported by secure authentication protocols, electronic signatures offer a reliable alternative to traditional handwritten signatures, thereby reducing the risk of unauthorised access or tampering.

Moreover, trust services contribute to legal compliance, given the widespread recognition of electronic signatures across many jurisdictions. This not only simplifies the compliance process for companies, but also reduces the risk of disputes related to the authenticity of documents.

Furthermore, these technologies facilitate seamless collaboration in today's globalised business landscape, allowing secure digital document exchange across diverse geographical boundaries.

Portugal

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.

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 Katie.Burrington@chambers.com