Legal 500
Country Comparative Guides 2025

Portugal
TMT

Contributor

Abreu Advogados

Ricardo Henriques

Partner | ricardo.henriques@abreuadvogados.com

José Maria Alves Pereira

Senior Associate | jose.a.pereira@abreuadvogados.com

Margarida Castillo Silva

Associate | margarida.c.silva@abreuadvogados.com

Pedro Hemsworth

Trainee Lawyer | pedro.hemsworth@abreuadvogados.com

This country-specific Q&A provides an overview of tmt laws and regulations applicable in Portugal.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Portugal: TMT

1. Software – How are proprietary rights in software and associated materials protected?

In Portugal, proprietary rights in Software can be protected under Copyright, in particular Decree-Law No. 252/94, of October 20.

Article 1 of this statute confers protection analogous to that conferred on literary works to all computer programmes with a creative character, determining for the purposes of this protection that the preliminary design material of the computer programme is equivalent to the computer programmes.

Thus, under Portuguese law, computer programmes and their associated preliminary materials will be protected provided they are creative.

The protection itself for computer programmes (software) under Article 2(1) of the referred statute, is for their expression in any form. The expression of the computer programme is understood to be the source code, which is the expression of the programme in the form of a text written in a programming language, and the object code, which is a text written in a 'machine' language.

Article 2(2) expressly excludes the protection of the ideas and principles underlying any element of the programme or its interoperability such as logic, algorithms or programming language.

Under Portuguese Copyright Law, the protection will be automatic from the moment the work, in this case the Software, is created (externalized). Nevertheless, it is possible to obtain a registration on the Software created, which will constitute a presumption of ownership of Copyright in favor of the registrant.

2. Software – In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

The general rule under Portuguese Copyright Law for works made on hire is that the copyright holder is presumed to be the intellectual creator or author, unless otherwise stipulated.

However, for computer programmes, the rule is reversed. Indeed, according to article 3(3) of Decree-Law No. 252/94, in the case of computer programmes that are made for hire, the copyright is presumed to be held by the recipient of the programme, unless otherwise stipulated or unless something else results from the purposes of the contract.

Thus, in Portugal, if a software is developed by a software developer, consultant or other party for a customer, it will be the customer who will own the copyright of software or computer programme (in the absence of any agreed contractual position).

3. Software – Are there any specific laws that govern the harm / liability caused by Software / computer systems?

Currently, besides the general rules of civil and criminal liability under Portuguese Civil Law, there are no specific laws that govern the harm / liability caused by Software / computer systems in Portugal. Nevertheless, on 23 October 2024, the EU approved Directive (EU) 2024/2853 on liability for defective products, thereby repealing Directive 85/374/EEC and broadening the concept of 'product' to explicitly include software.

4. Software – To the extent not covered by (4) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

Yes. In Portugal there is Law No. 82/2021, of November 30, which establishes the procedures for monitoring, controlling, removing and preventing access in the digital environment to content protected by copyright and related rights, as well as the administrative procedure to be adopted in the event of unlawful making available of protected content, including the obligations, in this context, of intermediary network service providers, defined in the statute on electronic commerce in the internal market.

There is also the Cybercrime Law (Law No. 109/2009, of September 15), transposing into national law Council Framework Decision 2005/222/JHA, of February 24, on

attacks against information systems and adapting domestic law to the Council of Europe Convention on Cybercrime.

5. Software Transactions (Licence and SaaS) – Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

No.

6. Software Transactions (License and SaaS) – Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

Yes. In Portugal, it is very typical for a software vendor to cap its maximum financial liability to a customer in a software transaction.

Even though a standardized market level of cap does not exist, usually vendors tend to cap their financial liability to the total amount paid for the software transaction or the amount so far paid by the customer over a given period of time (usually 12 months).

7. Software Transactions (License and SaaS) – Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

Confidentiality breaches – it depends on what is agreed, in particular if there is either a specific NDA or penalty clause, but typically confidentiality breaches are included in the financial cap on the software vendor's liability.

Data protection breaches – it depends on what is agreed, but typically this is excluded from the financial cap on the software vendor's liability.

Data security breaches (including loss of data) – it depends on what is agreed, but typically this is excluded from the financial cap on the software vendor's liability.

IPR infringement claims – this is typically excluded from the financial cap on the software vendor's liability.

Breaches of applicable law – it depends on what is agreed, but typically this is excluded from the financial cap on the software vendor's liability.

Regulatory fines – it depends on what is agreed, but typically this is excluded from the financial cap on the software vendor's liability.

Wilful or deliberate breaches – in case general contractual clauses are at stake, under Portuguese Law on general contractual clauses (Decree-Law No. 446/85, of October 25), clauses excluding or limiting liability for default, delay or defective performance in the event of intent or serious misconduct are absolutely prohibited. This means that wilful or deliberate breaches should always be excluded from the financial cap on the software vendor's liability.

8. Software Transactions (License and SaaS) – Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

Although there are mechanisms for software source codes to be held in escrow, this not a very common practice in Portugal, particularly where the nature of the contract/product does not advise the adoption of such robust safeguards. In the context of more complex operations, the use of escrows has been increasing.

Nevertheless, the typical escrow provider in Portugal is ASSOFT (Portuguese Software Association).

9. Software Transactions (License and SaaS) – Are there any export controls that apply to software transactions?

Yes, there are.

In Portugal, the export controls on software transactions are made under the 'dual-use and technologies' regime provided for in Regulation (EC) 2021/821 and Decree-Law No. 130/2015, of Jully 9. According to these statutes, dual-use goods and technologies are any goods,

including software and technology, which can be used for both civil and military purposes, including all goods which can be used for non-explosive purposes or in any way assist in the manufacture of nuclear weapons or nuclear explosive devices.

Operators involved in export transactions of such goods should apply for their Export Licenses and pay particular attention to any unusual procedures (in international trade transactions) by their customers, as well as to the final destination and end-use of the goods and technologies to be exported.

10. IT Outsourcing – Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

There are no specific regulations under Portuguese law which govern IT outsourcing transactions.

11. IT Outsourcing – Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

The outsourcing of services by a company is a reasonable ground for collective dismissal or extinction of the employment position. Specifically, it is part of the concept of structural ground set out in paragraph 2(b) of Article 359 of the Labour Code, *i.e.* for reasons of '*economic and financial unbalance, change of activity, restructuring of the production organization or replacement of dominant products*', as long as it is duly justified and complies with the legally stipulated procedure.

However, with the most recent amendments to the Labor Code, in force since May 2023, Article 338-A has forbidden the outsourcing of services, stating that '*it is not allowed to resort to the acquisition of external services from a third party to meet the needs that were ensured by an employee whose contract was terminated in the previous 12 months by collective dismissal or dismissal for termination of employment*', which turns out to be contradictory regarding the existing rules on the grounds for collective dismissal and termination of employment.

In addition, the breach of this provision constitutes a very serious administrative offense imputable to the beneficiary of the acquisition of services, which may lead to a penalty the amount of which varies according to the turnover of the company and degree of guilty.

Since then, the incorporation of this provision in the Labor Code has been subject of discussion, namely regarding its constitutionality, opposing, of course, two principles that collide in this matter: the right to private property and freedom of enterprise against the principle of human dignity and job security, both constitutionally provided.

12. Telecommunications – Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

The main law governing electronic communications is Law No. 16/2022, of August 16 (Electronic Communications Law), which resulted from the transposition of Directives 98/84/EC, 2002/77/EC and (EU) 2018/1972 (European Electronic Communications Code). This law establishes the legal regime applicable to electronic communications networks and services, associated facilities and services, the management of radio spectrum and numbering resources, as well as certain aspects of terminal equipment, and defines the competences of the national regulatory authority (NRA) and other competent authorities in these areas.

In addition to the Electronic Communications Law, certain matters are regulated by *lex specialis*, such as, among others, the following:

- Law No. 41/2004, of August 18, concerning the processing of personal data and the protection of privacy in electronic communications (hereinafter 'E-Privacy Law').
- Decree-Law No. 151-A/2000, of July 20, which establishes the regime applicable to the licensing of radiocommunications networks and stations and the supervision of the installation of such stations and the use of the radio spectrum, as well as the definition of the principles applicable to radio fees, the protection of exposure to electromagnetic radiation and the sharing of radiocommunications infrastructures.
- Law No. 99/2009, of September 4, which establishes the regime applicable to administrative offences in the communications sector. This law defines the responsibilities, the factors for determining the applicable sanction, as well as the amounts of the fines depending on the offence in question.

- ANACOM, as the national regulatory authority, issues and approves certain Regulations that should also be considered.

13. Telecommunications – Please summarise any licensing or authorisation requirements applicable to the provision or receipt of telecommunications services in your country. Please include a brief overview of the relevant licensing or authorisation regime in your response.

All entities wishing to provide public telecommunications services or operate a public telecommunications network must be registered with, and have obtained a License from, ANACOM, in accordance with Decree-Law No. 151-A/2000, of July 20, in its current reading.

The use of a radio communications network to provide or operate public telecom services requires prior obtaining of a radio licence, which must contain, in particular:

- Identification of the holder;
- Purpose for which the license is granted;
- Date of issue;
- Duration;
- Technical parameters applicable to all stations comprising the network;
- Number and location of stations comprising the network, where applicable.

The use of stations that are part of a licensed radio communications network does not require an autonomous licence, except in the cases singled out by ANACOM.

The use of stations that are not part of a radio communications network to provide or operate public telecom services is subject to licensing, which must contain:

- Identification of the holder;
- Purpose for which the license is granted;
- Date of issue;
- Duration;
- Specific technical parameters for each station, within the network or service to which it belongs;
- Location of the station, where applicable.

Interested parties must submit an application to ANACOM completed in accordance with the instructions provided by ANACOM.

Network or station licences are transferable. Holders shall notify ANACOM in advance of their intention to transfer such licences and the conditions of the transfer.

Licences shall be valid for a period of five years, automatically renewable for equal periods, unless ANACOM gives written notice of its decision not to renew.

In any case, licences may be revoked in the following cases:

- Failure to pay the license fees due to ANACOM for two consecutive years;
- At the request of the holder.

14. Telecommunications – Please summarise the principal laws (present or impending) that govern access to communications data by law enforcement agencies, government bodies, and related organisations. In your response, please outline the scope of these laws, including the types of data that can typically be requested, how these laws are applied in practice (e.g., whether requests are confidential, subject to challenge, etc.), and any legal or procedural safeguards that apply.

Law No. 32/2008, of July 17, regulates the storage and transmission of traffic and location data relating to natural persons and legal persons, as well as related data necessary to identify the subscriber or registered user, for the purposes of investigating, detecting and prosecuting serious crimes by the competent authorities.

Providers of publicly available electronic communications services or of a public communications network shall retain, in accordance with this law, the following categories of data:

- Data necessary to find and identify the source of a communication;
- Data necessary to find and identify the destination of a communication;
- Data necessary to identify the date, time and duration of a communication;
- Data necessary to identify the type of communication;
- Data necessary to identify the telecommunications equipment of users, or what is considered to be their equipment;
- Data necessary to identify the location of mobile communication equipment.

Data relating to the civil identification of subscribers or users of publicly available communications services or of

a public communications network, the IP address assigned to the source of a connection and other basic data shall be stored for a period of one year from the date of completion of the communication. Traffic and location data may only be stored, in this context, upon judicial authorisation.

Regarding data protection and security, telecom providers shall:

- Keep the data in such a way it can be transmitted immediately, upon reasoned order of a judge, to the competent authorities;
- Ensure that the data kept are of the same quality and subject to a level of protection and security no lower than that of other data (e.g., content data) on the network;
- Take appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure;
- Take appropriate technical and organisational measures to ensure that only specially authorised persons have access to data;
- Destroy the data at the end of the retention period, except for data that has been preserved by order of the judge;
- Destroy data that has been preserved, when so ordered by a judge.

With the exception of data relating to the name and address of subscribers, data stored under this Law shall remain encrypted from the start of their storage and shall only be unencrypted for the purposes of transmission, in accordance with this law, to the competent authorities.

Appropriate technical and organisational measures to ensure a level of security shall be implemented taking into account the most advanced techniques, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

The content of the preceding paragraphs shall not either decrease compliance with the principles and rules relating to the quality and safeguarding of the confidentiality and security of data laid down in Regulation (EU) 2016/679, of April 27, and in Laws No.41/2004, of August 18, 46/2018, of August 13, and 58/2019, of August 8, and respective regulations.

The transmission of data stored under this statute may only be authorised by a reasoned order of the investigating judge upon request by the Public Prosecutor's Office if there are reasons to believe that the measure is indispensable for the discovery of the truth or that the evidence would otherwise be impossible or very difficult to obtain in the context of the investigation, detection and prosecution of serious crimes.

The retention of data revealing the content of communications, in turn, is prohibited, with the exception of two situations:

1. Under Law No. 41/2004, when subscribers have given their prior consent in accordance with the applicable Personal Data Protection legislation or storage is strictly necessary for the provider to provide an information society service expressly requested by the subscriber or user; and
2. Criminal procedural law on the interception and recording of communications as priorly authorized by an investigating judge.

15. Mobile communications and connected technologies – What are the principle standard setting organisations (SSOs) governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

The main SSO in the world is the International Organization for Standardization (ISO), which sets international standards for the telecommunications sector in general, but also for newer connected technologies, such as digital health or autonomous vehicles.

A few examples of relevant standards from this organization for these purposes are class 33 of ISO, which has standards for telecommunication systems, mobile services, integrated services digital network (ISDN), Electromagnetic compatibility (EMC), just to name a few.

Additionally, ISO also holds certifications regarding digital health (ISO/TR 11147:2023), as well as connected and autonomous vehicles (ISO 22737:2021).

For mobile communications, there is also another relevant SSO, which is the European Telecommunications Standards Institute – ETSI. This SSO has specific standards for Internet of Things (IoT), 5G, eHealth and Smart Grids and Meters.

Finally, another relevant SSO for this purpose is

International Telecommunication Union Telecommunication Standardization Sector (ITU-T). This organization has specific standards regarding several telecommunication issues.

16. Mobile communications and connected technologies – How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

Technical standards for this purpose have tremendous impact on the development of connected technologies, since they are seen by end-clients (both companies and consumers) as a quality stamp for this sector.

As a matter of fact, these standards are usually complex to comply with, which means that certification with one of the standards of these 3 SSOs has tremendous market value.

Additionally, meeting these standards can ultimately increase interoperability between devices, which directly impacts the development of connected technologies.

17. Data Protection – Please summarise the principal laws (present or impending), if any, that that govern data protection, including a brief explanation of the general purpose of those laws.

The legal framework for personal data protection in Portugal is that resulting from the direct application of the GDPR. In turn, one shall consider Law No. 58/2019, of August 8, which ensures the implementation in Portugal of the GDPR (hereinafter 'Portuguese Data Protection Law').

Apart from the GDPR and the Portuguese Data Protection Law, which set the general framework applicable to the processing of personal data, certain situations are governed by *lex specialis*, among which we would like to point out:

- Law No. 41/2004, August 18, concerning the processing of personal data and the protection of privacy in electronic communications (hereinafter 'E-Privacy Law'). This law covers the processing of personal data for e-marketing purposes, as well as the use of cookies and similar technologies.
- Law No. 7/2009, February 12 (hereinafter 'Portuguese Labor Code'), which provides for special rules for the processing of personal within a labor relationship.
- Law No. 59/2019, of August 8, which transposes Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016). In general, this law sets forth the rules on the processing of personal data by competent authorities for the purpose of prevention, detection, investigation or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

18. Data Protection – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

As per article 83 of the GDPR and the Portuguese Data Protection Law, the maximum fine ranges from EUR 10m to EUR 20m or, in the case of an undertaking, 2% to 4% of the total worldwide annual turnover of the preceding financial year, respectively, whichever is higher.

The amount of an administrative fine will vary depending on the circumstances of each individual case and shall be effective, proportionate and dissuasive.

The European Data Protection Board has issued Guidance on the calculation of fines in its Guidelines 04/2022 of 12 May 2022.

The Portuguese Data Protection Law introduces a different frame of penalties for infringing entities, setting a criteria based on the company's economic size. According to Article 37, small and medium-sized enterprises are subject to a maximum administrative penalty of EUR 2m, or 4% of their total worldwide annual turnover in the preceding financial year, whichever is higher. However, the CNPD issued a deliberation deciding on the inapplicability of this provision, as it violates the GDPR directly.

19. Data Protection – Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

When entered into by Portuguese companies, technology contracts commonly reference both the EU GDPR and the Portuguese Data Protection Law, where applicable. While the GDPR applies directly in Portugal, its broad territorial scope also extends to companies outside the EU that process personal data of individuals located within the EU. As the GDPR is widely regarded as an international benchmark for data protection, it is often the sole

normative reference in such contracts.

20. Cybersecurity – Please summarise the principal laws (present or impending), if any, that that govern cybersecurity (to the extent they differ from those governing data protection), including a brief explanation of the general purpose of those laws.

Portugal has been strengthening its cybersecurity legal framework through the transposition and implementation of European legislation.

Notably, Law No. 46/2018, of August 13, establishes the legal regime for cyberspace security, transposing the EU's NIS 1 Directive (Directive (EU) 2016/1148). This law sets out security requirements for essential service operators and digital service providers and imposes mandatory incident notification obligations in the event of significant cybersecurity breaches.

Portugal is in the process of transposing the NIS 2 Directive (Directive (EU) 2022/2555), which aims to further harmonize cybersecurity obligations across the EU by introducing stricter requirements and expanding the scope of regulated entities. The Directive imposes new responsibilities and accountability measures, including personal liability for members of the governing and administrative bodies of essential and important entities in cases of non-compliance with the cybersecurity framework.

The NIS 2 Directive is complemented by the CER Directive (Directive (EU) 2022/2557), which intends to reinforce the resilience of critical entities. Portugal has recently approved its national transposition law, Decree-Law No. 22/2025, of March 19, consolidating the resilience of critical entities through the imposition of the following core obligations on critical entities: (i) carry out risk assessments; (ii) drawing up and implementing a Resilience Plan; (iii) appointment of a liaison officer; (iv) draw up procedures for reporting incidents that significantly disrupt service provision; and (v) request background checks.

The financial sector is set to benefit from the DORA Regulation (Regulation (EU) 2022/2554). The main objective of the DORA Regulation is to achieve a high common level of digital operational resilience. This comprehensive regulation introduces key obligations for financial entities regarding the security of networks and information systems that underpin their operations.

In October 2024, the EU introduced the Cyber Resilience Act (Regulation (EU) 2024/2847), thus providing a robust level of cybersecurity for products with digital elements to be placed on the internal market. Although directly applicable in Portugal, this Regulation requires the adoption of national implementing legislation for specific provisions that empower the national legislator (*e.g.*, provisions on penalties).

Lastly, the Cybersecurity Act (Regulation (EU) 2019/881) establishes the 'European cybersecurity certification framework' and provides a harmonised standard for cybersecurity certification across the EU. Portugal has implemented this Regulation through Decree-Law No. 65/2021, of July 30, designating the CNCS as the National Cybersecurity Certification Authority, responsible for implementing a national cybersecurity certification framework.

21. Cybersecurity – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable cybersecurity laws?

Cybersecurity legislation within the EU provides a range of sanctions applicable to infringing entities. Regarding administrative sanctions, currently the Cyber Resilience Act sets the highest penalty of EUR 15 000 000, or if the offender is an undertaking, up to 2,5 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

As for the NIS2 Directive, although its transposition into national law is still underway, the expected maximum administrative fine for essential entities is EUR 10 000 000, or 2% of their total worldwide annual turnover, again applying the higher of the two. These sanctions aim to ensure robust enforcement of cybersecurity obligations across the EU.

22. Artificial Intelligence – Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

The body responsible for supervising the rules on artificial intelligence has not yet been designated in Portugal.

However, the bodies responsible for supervising compliance with European Union legislation protecting fundamental rights have already been designated and notified to the European Commission. These are:

- Autoridade Nacional de Comunicações (ANACOM);

- Inspeção-Geral das Finanças (IGF);
- Gabinete Nacional de Segurança (GNS);
- Entidade Reguladora para a Comunicação Social (ERC);
- Inspeção-Geral da Defesa Nacional (IGDN);
- Inspeção-Geral dos Serviços de Justiça (IGSJ);
- Polícia Judiciária (PJ);
- Inspeção-Geral da Administração Interna (IGAI);
- Inspeção-Geral da Educação e Ciência (IGEC);
- Entidade Reguladora da Saúde (ERS);
- Autoridade de Segurança Alimentar e Económica (ASAE);
- Inspeção-Geral do Ministério do Trabalho, Solidariedade e Segurança Social (IGMTSSS);
- Autoridade para as Condições do Trabalho (ACT);
- Entidade Reguladora dos Serviços Energéticos (ERSE).

23. Artificial Intelligence – Please summarise the principal laws (present or impending), if any, that that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

The deployment and use of artificial intelligence is governed by the European Union's Artificial Intelligence Act.

In addition, Law No. 27/2021, of May 17, which establishes the Portuguese Charter of Human Rights in the Digital Age. Article 9 refers to the use of artificial intelligence and robots providing that their use must be guided by respect for fundamental rights, ensuring a fair balance between the principles of explainability, security, transparency and accountability, taking into account the circumstances of each specific case and establishing processes aimed at avoiding any prejudice and forms of discrimination. Furthermore, decisions that significantly impact the interests of recipients and are made using algorithms must be communicated to stakeholders, be subject to appeal and be auditable.

24. Artificial Intelligence – Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI (including agentic AI)?

Besides the rules established the European Union's Artificial Intelligence Act (*e.g.* Article 53), there are no specific rules governing foundation models, including large language models and generative AI systems.

25. Artificial Intelligence – Do technology contracts in your jurisdiction typically contain either mandatory (e.g. mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

It is still not very common, in Portugal, for contracts to contain provisions dealing with AI risk. However, in face of the new rules on Artificial Intelligence provided in the AI Act, economic operators have begun displaying increased interest in addressing AI risks and limitations in technology-related contracts. We expect this to become standard practice in the coming years.

26. Artificial Intelligence – Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

With the emergence of generative AI tools, there has been a growing concern about the risks inherent in the results generated by this type of tool in terms of copyright, as well as the respective attribution of copyright ownership.

In Portugal, provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems, are becoming more common in technology contracts in general, but are not yet widely used.

27. Blockchain – What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

Portugal has implemented the EU Regulation 2022/858 of the European Parliament and of the Council, dated May 30th, 2022 through the Decree-Law No. 66/2023, of August 8. Under the new regime, the Portuguese Securities Market Commission (CMVM) has been designated as the competent national authority for supervising matters related to the Blockchain (distributed ledger technology – DLT).

Moreover, the Bank of Portugal is the Portuguese competent authority responsible for registering entities

intending to act as virtual assets service providers and verifying compliance with the legal and regulatory provisions governing the prevention of money laundering and terrorist financing ('AML/CFT').

Decree-Law No. 67/2021, of July 30, sets the framework for the creation of 'Technological Free Zones' (ZLT's). ZLT's are physical environments for testing, geographically located, in a real or near-real environment, designed for their promoters to test innovative technology, products, services and processes in a safe manner, with the support and monitoring of the respective competent authorities. This Decree-Law does not create the ZLT's right away but determines the conditions for their creation with the aim of setting up several ZLT's in Portugal, each of which is specially geared towards certain technologies or sectors and thus contributes to boosting Portugal's regions by leveraging their specific characteristics.

Furthermore, the European Securities and Markets Authority (referred to as 'ESMA') will assume a pivotal role in ensuring regulatory harmonization and will acquire comprehensive insights into noteworthy cryptocurrency providers in accordance with the implemented MiCA regulation. Lastly, the European Banking Authority (abbreviated as 'EBA') will oversee issuers of noteworthy asset-referenced tokens and substantial stablecoins.

28. Search Engines and Marketplaces – Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

Search engines and marketplaces, in Portugal, are currently regulated by Regulation (EU) 2022/2065 of the European Parliament and of the Council, of 19 October 2022 ('Digital Services Act' or 'DSA'), which has become fully enforceable and applicable on 17 February 2024. This Regulation introduces new obligations for online platforms to reduce harm and tackle online risks, introduces solid protection of online users' rights and establishes a new single transparency and accountability framework for digital platforms.

Search engines are further regulated by Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 ('Digital Markets Act' or 'DMA') which is fully applicable since 2 May 2023. The Digital Markets Act does not apply to all digital platforms, but only to those qualified as '*core platform services*' ('CPS'), which includes services such as search engines, web browsers, virtual assistants, video sharing platforms, among others. The scope of the Digital Markets Act is further limited to platforms designated as gatekeepers. The gatekeeper must (a) have a size that impacts the EU internal market; (b) provide a core platform service which is an important gateway for business users to reach end users; and (c) enjoy an entrenched and durable position in the market. The Digital Markets Act thus establishes a system of prohibitions and multiple positive obligations for gatekeepers.

Some local legislation is also applicable to marketplaces, such as:

- Decree-Law No. 84/2021, of October 18, which regulates consumer rights in the purchase and sale of goods, digital content and services. This Decree-Law provides that the online marketplace provider who, acting for purposes related to his activity, is a contractual partner of the trader who makes the good, digital content or service available is jointly and severally liable to the consumer for the lack of conformity of those under the law (Article 44). This statute also provides for a special information duty for the online marketplace provider who is not a contractual partner of the trader providing the good, digital content or service, being required to make certain information available to consumers.
- Decree-Law No. 24/2014, of February 14, on consumer rights in distance and off-premises contracts. This statute provides for specific additional information requirements for contracts concluded on online marketplaces applicable to online marketplace providers (Article 4a), as well as specific rules applicable to situations where the online marketplace provider offers access to consumer reviews (Article 4b).

29. Social Media – Please summarise the principal laws (present or impending), if any, that govern social media and online platforms, including a brief explanation of the general purpose of those laws?

In Portugal the main law governing social media is Decree-Law No. 7/2004, of January 7 (which transposed to the Portuguese legal framework the e-Commerce Directive).

With the entry into force of the DSA, although Decree-Law No. 7/2004, of January 7 has not been expressly repealed, as far as the Safe Harbor regime is concerned, the DSA applies in full. According to the latter, in order to be exempted from liability and thus benefit from the Safe-

Harbor regime, intermediary services providers, in particular hosting service providers shall: (i) not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or (ii) upon obtain actual knowledge or awareness of illegal activities or content, act fast to remove or disable access to the content (Article 6 of the DSA).

In the event of removal of content or disabling access to content on the grounds of illegal activity or because they do not follow the terms and conditions of the service, the DSA set forth an obligation to providers of hosting services to provide a clear and specific statement of reasons to the affected recipient or user on the ground that the information uploaded by it is illegal or incompatible with the terms and conditions. The same applies when suspension or termination of the recipient of the service's account is applied (Recital 54 and Article 17 of the DSA).

In addition, with regard to content moderation obligations, we must also consider other general provisions, such as the Portuguese Criminal Code, Industrial Property Code, and the Portuguese Advertising Code.

In respect of copyright-infringing content, Article 175-C (1)(a), (b) and (c) of the Portuguese Copyright and Related rights Code (Decree-Law No. 63/85, of March 14), which transposes Article 17(4) (a), (b) and (c) of Directive (EU) 2019/790 ('DSM' Directive), stipulates certain obligations (best efforts, content blocking and stay down) for online content-sharing service provider platforms that host and make available to the public large quantities of copyrighted materials, in order to avoid a direct liability for copyright-infringing user-uploaded content. This means that the 'Safe-Harbor' privilege conferred by e-Commerce Directive, no longer applies in copyright matters.

Lastly, one shall also consider the provision of the DMA which also applies to (large) social networking sites and imposes several obligations on them (please refer to question No. 28).

30. Social Media – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable online safety laws?

Fines for breaching the DMA (although not specifically related only to online safety) can ascend to 20% of the company's annual worldwide turnover. Fines for Breaches of the DSA can also ascend to 6% of the company's annual worldwide turnover. These are the highest fine caps in this context.

31. Spatial Computing – Please summarise the principal laws (present or impending), if any, that govern spatial computing, including a brief explanation of the general purpose of those laws?

Spatial computing is a term that comprises a variety of new technologies, such as augmented, extended, and virtual reality, along with the metaverse. These technologies are not expressly statutorily regulated in Portugal. However, one cannot say that spatial computing is unregulated in Portugal, as these technologies are subject to general civil and criminal law, as well as data protection regulations and cybersecurity legislation.

The European Commission has supported an EU initiative on Web 4.0 and virtual worlds, promoting the dialogue between local authorities and the EU parliament with the aim of supporting EU's role as a major player in this nascent market.

Apart from such initiative, no legislation has been proposed yet to regulate the inherent risks posed by digital twins and natives in the metaverse, which extend beyond the digital sphere and threaten intellectual property rights, personality rights, property rights, among others.

32. Quantum Computing – Please summarise the principal laws (present or impending), if any, that govern quantum computing and/or issues around quantum cryptography, including a brief explanation of the general purpose of those laws?

Quantum computing is likewise a term that comprises a variety of applications. It is a type of computing that leverages quantum mechanics to solve complex problems that are intractable for classical computers. It utilizes quantum phenomena like superposition and entanglement to process information in fundamentally different ways, potentially offering exponential speedups for specific tasks.

While some jurisdictions have begun approaching the regulation of quantum computing-based applications,

Portuguese authorities have not issued any documentation specific to them.

The risks and challenges brought by quantum computing shall, then and in any case, be addressed through the application of non-specific software legislation, which includes terms for copyright and other proprietary interests.

33. Datacentres – Does your jurisdiction have any specific regulations that apply to data centres?

As artificial intelligence continues to revolutionize productivity, innovation, and profitability, data centres have become its essential infrastructure – both its motor and fuel. In recognition of their growing environmental impact, data centres are now subject to specific transparency and reporting obligations under the Energy Efficiency Directive (Directive (EU) 2023/1791), as recast in 2023.

Portugal has implemented these obligations through Decree-Law No. 84/2024, of November 4, which partially transposes both the Directive and Commission Delegated Regulation (EU) 2024/1364. This legislation applies to data centres located in Portugal with an installed IT power demand of at least 500 kW.

Additionally, the Decree-Law also defines incentives for data centres located in Portugal that wish to adopt the practices set out in the European code of conduct on energy efficiency in data centres.

The Directorate-General for Energy and Geology (DGEG) is designated as the national authority responsible for overseeing compliance, publishing performance data, and ensuring enforcement.

34. General – What are your top 3 predictions for significant developments in technology law in the next 3 years?

- Considering the framework established for primary and secondary uses of health data, the European Health Data Space Regulation, which has already entered into force, is expected to greatly impact the handling of relevant personal data in the healthcare sector.
- The EU Space Act, the proposal of which has just been introduced late June 2025, is likely to impact cybersecurity and cyber resilience standards of satellite and telecom infrastructures (and related legislation).
- The EU Data Act, which has already entered into force and will become applicable in September 2025, has been suggested as strengthening EU's non-personal data landscape.

35. General – Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

Not usually although we've notices it is becoming a tendency in the Portuguese jurisdiction, also due to ESG legislation from the European Union, such as the ESG Directive (Directive (EU) 2022/2464, of 14 December 2022) and EU Delegated Regulation 2023/2772, of 31 July, 2023.

In any case, we expect the increasing concerns with sustainability issues, as well as the EU's legislative plan for this sector will impact the inclusion of said clauses in technology contracts, eventually until such clauses become standard in these sorts of contracts.

Contributors

Ricardo Henriques
Partner
ricardo.henriques@abreuadvogados.com

José Maria Alves Pereira
Senior Associate
jose.a.pereira@abreuadvogados.com

Margarida Castillo Silva
Associate
margarida.c.silva@abreuadvogados.com

Pedro Hemsworth
Trainee Lawyer
pedro.hemsworth@abreuadvogados.com