Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Artificial Intelligence 2026

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

Portugal: Law and Practice

Jorge Silva Martins, João Carminho and Leonor Gambôa Machado
MFA Legal & Tech

PORTUGAL

Law and Practice

Contributed by:
Jorge Silva Martins, João Carminho and Leonor Gambôa Machado
MFA Legal & Tech

Contents

1. Legal Framework p.5
1.1 General Legal Background p.5

2. Commercial Use of AI p.6
2.1 Industry Use p.6
2.2 Involvement of Governments in AI Innovation p.6

3. AI-Specific Legislation and Directives p.7
3.1 General Approach to AI-Specific Legislation p.7
3.2 Jurisdictional Law p.7
3.3 Jurisdictional Directives p.8
3.4 EU AI Act p.8
3.5 US State Law p.8
3.6 Data, Information or Content Laws p.8
3.7 Proposed AI-Specific Legislation and Regulations p.9

4. Case Law p.9
4.1 Precedent-Setting Judicial Decisions p.9

5. AI Regulatory Oversight p.10
5.1 Regulatory Agencies p.10
5.2 Regulatory Directives p.10
5.3 Enforcement Actions p.10

6. Standard-Setting Bodies p.10
6.1 National Standard-Setting Bodies p.10
6.2 International Standard-Setting Bodies p.11

7. AI and the State p.11
7.1 Government Use of AI p.11
7.2 Judicial Decisions p.11
7.3 National Security p.12

8. Generative AI p.12
8.1 Generative AI: Key Legal Issues and Regulatory Approaches p.12

9. Legal Tech p.13
9.1 AI in the Legal Profession and Ethical Considerations p.13

10. Liability for AI p.13
10.1 General Theories of Liability p.13
10.2 Regulatory Approaches to Liability for AI p.13

11. Agentic AI Systems and Autonomous Decision-Making p.14
11.1 Agentic AI Systems: Legal Framework and Governance p.14
11.2 Liability Allocation for Autonomous AI Systems p.14

12. Specific Legal Issues With AI p.15
12.1 Algorithmic Bias and Fairness p.15
12.2 Biometric Technologies and Emotion Recognition p.15
12.3 Deepfakes and Synthetic Media p.15
12.4 Transparency and Disclosure p.16

13. AI Procurement and Supply Chain Accountability p.17
13.1 AI Procurement Standards and Contracting p.17
13.2 AI Supply Chain Accountability and Due Diligence p.17

14. Employment p.17
14.1 Hiring and Termination Practices p.17
14.2 Employee Evaluation and Monitoring p.18

15. AI in Industry Sectors p.18
15.1 Digital Platform Companies p.18
15.2 Financial Services p.19
15.3 Healthcare p.19
15.4 Autonomous Vehicles p.20
15.5 Retail and Consumer p.20
15.6 Industrial AI and Robotics p.20

16. Intellectual Property p.21
16.1 IP Protection for AI Assets p.21
16.2 AI as Inventor/Author p.21
16.3 Copyright and AI Training Data p.22
16.4 AI-Generated Works of Art and Works of Authorship p.22
16.5 Foundation Models and Open-Source AI: IP Considerations p.23

17. Data Protection p.23
17.1 AI Training and Data Protection p.23
17.2 AI Deployment and Data Subject Rights p.24
17.3 AI Data Governance and Cross-Border Transfers p.24

18. Antitrust p.25
18.1 Emerging Antitrust Issues in AI p.25

19. Cybersecurity p.25
19.1 Applicability of Cybersecurity Legislation to AI p.25

20. ESG p.26
20.1 ESG Dimensions of AI p.26

21. AI Governance and Compliance p.26
21.1 AI Governance Frameworks and Implementation p.26

MFA Legal & Tech is a Portuguese boutique law firm combining senior expertise in tax, white-collar crime, compliance, technology and digital regulation, with a strong focus on highly regulated and innovation-driven sectors. Built by lawyers with extensive international and multidisciplinary experience, the firm is structured to support clients on business-critical legal, operational and governance challenges requiring integrated strategic advice. The Technology, Innovation & Regulatory practice comprises seven professionals and supports domestic and international clients across the full digital ecosystem, including electronic communications, e-commerce, intellectual property, artificial intelligence, cybersecurity, privacy and data protection, digital platforms, consumer law, blockchain and other emerging technologies. The team is regularly involved in regulatory investigations, strategic transactions, digital transformation initiatives, technology contracting, public policy projects and the implementation of governance and compliance frameworks under evolving EU digital regulation.

Authors

Jorge Silva Martins is partner and head of the Technology, Innovation & Regulatory practice at MFA Legal & Tech. He advises leading national and international clients on regulatory, transactional and strategic matters involving digital infrastructure, electronic communications, cybersecurity, data protection, artificial intelligence and blockchain. He is particularly recognised for advising on cross-border mandates, digital transformation projects and the design and implementation of regulatory and governance frameworks in highly regulated sectors. Jorge is vice-president of ACEPI, Portugal's largest digital economy association, and a board member of the AI Lab at the Lisbon School of Law.

João Carminho is a managing associate in the Technology, Innovation & Regulatory practice at MFA Legal & Tech. His practice focuses on the operational implementation of digital regulation, including privacy, intellectual property, cybersecurity and technology contracting. João is regularly involved in regulatory investigations, pre-litigation strategy and administrative and judicial proceedings, while also supporting the deployment of AI governance programmes, digital compliance frameworks and strategic technology projects across sectors.

Leonor Gambôa Machado is an associate in the Technology, Innovation & Regulatory practice at MFA Legal & Tech. Her practice focuses on consumer law, data protection, digital regulation and emerging technologies, with particular experience in projects involving artificial intelligence, digital platforms and online business models. She is also a researcher at the NOVA Consumer Lab, where she has been involved in academic and policy work on consumer protection, digital markets and technology regulation since 2021.

MFA Legal & Tech

Edifício Jean Monnet
Largo Jean Monnet, No 1, piso 2 | 1250-130
Lisboa
Portugal

Tel: + 351 211 372 676
Email: fc@mfalegal.pt
Web: www.mfalegal.pt

1. Legal Framework

1.1 General Legal Background

The regulatory landscape for artificial intelligence in Portugal is currently characterised by a combination of directly applicable EU legislation and the continued reliance on established legal frameworks not originally designed with AI in mind.

At EU level, the AI Act marks a structural shift in how AI is governed, introducing a risk-based model that differentiates between prohibited, high-risk and lower-risk systems. While the Regulation entered into force in 2024, its phased implementation creates a transitional compliance period during which organisations must progressively adapt their governance, technical and contractual frameworks.

Portugal has not yet adopted bespoke AI legislation, reflecting its traditionally alignment-driven approach to EU digital regulation. AI systems are therefore primarily governed through horizontal regimes – particularly data protection, intellectual property, consumer protection and product safety – interpreted in light of evolving EU standards. For most organisations, legal risk arises less from the absence of regulation and more from the complexity of applying already existing rules to novel technological contexts.

The application of these regimes varies depending on the type of AI. Predictive AI raises concerns around automated decision-making and discrimination; generative AI introduces risks related to content creation, intellectual property and misinformation; and, more advanced, agentic AI challenges traditional concepts of liability and human control.

Key areas of relevance include:

- Data Protection and Privacy: AI systems, particularly those relying on large-scale datasets, raise compliance challenges under the General Data Protection Regulation, notably regarding lawful basis, purpose limitation and transparency in "black box" models. The Portuguese Data Protection Authority (CNPD) adopts a comparatively interventionist stance, especially on biometric data and cross-border flows, and has supported international initiatives addressing risks associated with AI-generated content, including as a signatory to the Joint Statement on AI-Generated Imagery and the Protection of Privacy dated 23 February 2026, co-ordinated by the International Enforcement Cooperation Working Group of the Global Privacy Assembly.
- Intellectual Property: AI has exposed structural limitations in existing IP regimes. While software and underlying models benefit from protection under EU law, the legal status of both training inputs and generated outputs remains uncertain.
- Contractual Frameworks: Contracts play a central role in managing AI-related risk, addressing not only liability and ownership but also training restrictions, audit rights, explainability and regulatory compliance, particularly in the context of general-purpose and third-party AI systems.
- Liability and Product Safety: The absence of AI-specific liability rules at national level is partially offset by evolving EU legislation. The revised Prod-

uct Liability Directive extends strict liability to digital and AI-enabled products, lowering the threshold for claims, particularly where AI is embedded in regulated products, and signalling a shift towards outcome-based accountability.
- Consumer Protection: AI systems used in consumer-facing contexts, such as recommendation engines, pricing tools or automated interactions, must comply with rules on transparency, fairness and misleading practices. Generative AI raises additional concerns around deceptive or synthetic content.
- Employment: The use of AI in recruitment and workforce management is subject to labour law constraints, particularly regarding discrimination, transparency and employee rights, which may limit automated decision-making.

Overall, the Portuguese framework reflects regulatory convergence rather than fragmentation, with AI governance emerging from the interaction between EU legislation and the adaptive interpretation of existing national legal regimes.

2. Commercial Use of AI

2.1 Industry Use

Artificial intelligence is no longer confined to experimental environments in Portugal and is increasingly embedded in the operational core of both private and public organisations. Adoption spans traditional machine learning systems, foundation models and large language models, retrieval-augmented generation architectures and, more recently, early agentic systems capable of autonomous task orchestration.

Traditional machine learning remains widely deployed in sectors such as telecommunications, financial services, energy, manufacturing and logistics, where predictive models are used for network optimisation, fraud detection, predictive maintenance, demand forecasting and operational efficiency. Portuguese telecommunications operators, utilities and industrial groups increasingly rely on these systems to optimise infrastructure management and reduce operational costs.

Foundation models and large language models have accelerated adoption across professional services, retail, healthcare and customer-facing businesses. Portuguese organisations are increasingly integrating LLM-based systems for document analysis, customer support, automated content generation, translation, summarisation and knowledge management. Law firms, banks and insurers are beginning to deploy internal generative AI environments trained on proprietary databases.

Retrieval-augmented generation systems are emerging as a preferred architecture in regulated sectors, particularly legal, healthcare, finance and public administration, as they allow organisations to combine generative capabilities with trusted internal datasets, reducing hallucination risks and strengthening auditability.

Agentic AI remains at an early stage but pilot deployments are emerging in workflow automation, procurement, compliance, IT support and customer interaction.

2.2 Involvement of Governments in AI Innovation

Portugal has adopted an innovation-enabling approach to artificial intelligence, combining public investment, policy incentives, digital-skills programmes, regulatory experimentation and strategic alignment with broader EU digital and industrial policy initiatives.

One of the main strategic instruments has been AI Portugal 2030, developed under the INCoDe.2030 initiative, which aims to strengthen digital skills, support AI adoption across economic sectors, attract talent, and foster research, entrepreneurship and technology transfer. This policy direction was further reinforced by the National Artificial Intelligence Agenda, approved by Resolution of the Council of Ministers No 2/2026, which establishes a more operational national framework focused on computing infrastructure, data access, public-sector adoption, business competitiveness, skills development, regulatory preparedness and responsible AI governance.

Public funding for AI innovation is channelled through multiple mechanisms, including the Recovery and

Resilience Plan, COMPETE 2030, innovation vouchers, digital innovation hubs and sector-specific funding programmes. These initiatives support start-ups, SMEs, universities, research centres and public-sector modernisation projects.

Portugal also participates in European data and research initiatives relevant to AI innovation, including HealthData@EU, while aligning national digital-health infrastructure with the emerging European Health Data Space framework.

From a regulatory perspective, Portugal is also expected to develop AI regulatory sandboxes and controlled testing environments as part of the implementation of the EU AI Act.

3. AI-Specific Legislation and Directives

3.1 General Approach to AI-Specific Legislation

Portugal adopts a hybrid, EU-driven regulatory philosophy towards AI, combining a risk-based framework with an innovation-enabling approach. This model is primarily shaped by the AI Act, which introduces harmonised rules across the EU and reflects a precautionary stance in high-risk contexts, balanced with support for technological development.

No standalone AI-specific legislation has yet been enacted at national level, nor are there advanced legislative proposals currently under discussion. Instead, Portugal has opted for regulatory alignment with EU instruments, complemented by national policy initiatives, most notably the National Artificial Intelligence Agenda, which sets the strategic framework for AI adoption in Portugal through 2030.

The regulatory framework distinguishes between AI capabilities and use cases based on risk. High-risk AI systems are subject to extensive obligations, including risk management, data governance, technical documentation, human oversight and conformity assessment. By contrast, general-purpose AI (GPAI) and foundation models are subject to transparency, documentation and governance requirements, with additional obligations where systemic risk is identified.

The AI Act does not regulate autonomy levels in abstract terms but operationalises control through human oversight requirements, ensuring that AI systems remain subject to meaningful human intervention, particularly where fundamental rights may be affected. This reflects a broader EU principle of "human-in-the-loop" governance.

3.2 Jurisdictional Law

Portugal has not enacted AI-specific legislation beyond the direct applicability of the AI Act, which entered into force in August 2024 and is being implemented on a phased basis, with certain obligations extending beyond the general application date of August 2026.

The AI Act establishes a comprehensive legal framework applicable to providers, deployers, importers and distributors of AI systems. Its scope is broad, covering both standalone AI systems and AI components embedded in products, with extraterritorial reach where systems are placed on the EU market or affect individuals within the EU.

Key obligations vary depending on the classification of AI systems:

- High-risk AI systems are subject to stringent requirements, including risk management systems, high-quality datasets, technical documentation, record-keeping, transparency, human oversight and cybersecurity measures.
- General-purpose AI (GPAI) and foundation models are subject to specific obligations, including the preparation of technical documentation, provision of information to downstream users, and, for models with systemic risk, additional requirements relating to risk mitigation, evaluation and incident reporting.
- Transparency obligations apply to certain AI systems, including those interacting with individuals or generating synthetic content, requiring disclosure of AI involvement.

Enforcement mechanisms are supported by national implementation measures, including the designation of competent supervisory authorities and the establishment of penalties for non-compliance.

3.3 Jurisdictional Directives

To date, Portuguese public authorities have not issued comprehensive, cross-cutting AI-specific soft law instruments governing the development or deployment of AI systems.

That said, sector-specific guidance is beginning to emerge, particularly in sensitive domains. In the judicial context, both European and national bodies have adopted non-binding instruments addressing the use of AI, emphasising its strictly auxiliary role, the need for effective human oversight and the preservation of fundamental rights, judicial independence and procedural fairness. These developments reflect a broader trend towards context-specific soft law, rather than horizontal guidance.

More generally, existing guidance issued by regulators – particularly in the areas of data protection and employee monitoring – may indirectly apply to AI systems, although it does not specifically address AI-related risks.

At institutional level, Portugal has also established a decentralised supervisory framework under Article 77 of the AI Act, designating multiple authorities responsible for overseeing compliance with EU rules protecting fundamental rights. While this framework is primarily enforcement-oriented, it is expected that these bodies will progressively contribute to the development of interpretative guidance and best practices within their respective areas of competence.

Public sector initiatives such as INCoDe.2030, the GuIA (a practical framework for ethical and responsible AI adoption developed by the former Portuguese Administrative Modernisation Agency), and the National Artificial Intelligence Agenda focus on digital skills, innovation, responsible AI adoption and risk assessment tools. While they are relevant policy and governance instruments, they do not currently constitute binding regulatory guidance.

3.4 EU AI Act

Portugal's approach to the implementation of the AI Act is closely aligned with the Regulation's phased application model, under which different categories of obligations become applicable at different points in time.

As a directly applicable Regulation, the AI Act does not require transposition. Portugal has, however, already adopted important institutional implementation measures, including the identification of national authorities responsible for the protection of fundamental rights under Article 77. In parallel, the government has publicly announced its intention to designate ANACOM as the national market surveillance authority and single point of contact under the AI Act, with a central coordination role across a broader set of sectoral regulators involved in the oversight of AI-related risks. However, at the time of writing, the formal implementing act confirming that designation has not yet been publicly identified.

Further implementation steps remain relevant, including the designation of notified bodies, the operationalisation of enforcement mechanisms and penalty regimes, and the development of practical compliance tools. The National Artificial Intelligence Agenda expressly anticipates measures in this area, including regulatory sandboxes, guidance on implementation of the AI Act, standards and national risk assessment tools.

3.5 US State Law

There is no applicable information in this jurisdiction.

3.6 Data, Information or Content Laws

Portugal has not introduced AI-specific amendments to data protection, copyright or content laws.

However, existing frameworks play a central role in regulating AI-related activities. Under the GDPR, AI-related data processing must comply with principles such as lawfulness, transparency, purpose limitation and data minimisation. No AI-specific processing rules have been adopted, although general provisions on automated decision-making and profiling are directly relevant.

Directive (EU) 2019/790, transposed into the Portuguese legal order by Decree-Law No 47/2023, of 19 June, establishes text and data mining exceptions that may support the extraction and analysis of protected content for machine learning and other computational purposes, subject to conditions and opt-out mechanisms. The application of these exceptions to commercial AI training remains highly fact-specific and legally complex.

No specific national rules address the legality of web scraping in the AI context. Its permissibility depends on the interaction between copyright, database rights, contractual restrictions, competition law and data protection rules.

Similarly, no dedicated regulatory framework exists for synthetic data. Its legal treatment depends on the methodology used, the possibility of re-identification, and whether the resulting datasets remain linked to identifiable individuals or protected source material.

3.7 Proposed AI-Specific Legislation and Regulations

At national level, there are no current legislative proposals specifically addressing AI.

Regulatory developments are expected to continue to originate at EU level, with the AI Act constituting the primary instrument. Ongoing discussions at EU level may further address issues such as systemic risk in foundation models, supply chain accountability and obligations for general-purpose AI providers.

Emerging areas, such as agentic AI systems and autonomous agents, are not yet specifically regulated, although they are likely to be captured within existing risk-based frameworks.

Portugal is expected to follow these developments closely.

4. Case Law

4.1 Precedent-Setting Judicial Decisions

Portuguese courts have not yet developed a consolidated body of case law specifically addressing artificial intelligence. However, AI-related disputes are beginning to emerge indirectly, particularly in the context of data protection, consumer protection and digital platform liability.

A notable trend is the increasing use of collective redress mechanisms against major technology companies, including Google, Apple, Sony, TikTok and Meta. These actions, often supported by third-party litigation funders and driven by active consumer associations, frequently raise issues that are directly relevant to AI systems, such as large-scale data processing, algorithmic decision-making and transparency obligations.

While several first-instance decisions were issued in 2024, the legal framework governing these proceedings remains in development. The next phase will likely see appellate courts clarifying key procedural aspects, including standing, admissibility of class actions, the role and independence of litigation funders, and the scope of data protection mandates. These developments are likely to shape the procedural landscape for future AI-related claims.

Separately, concerns around the use of AI within the judiciary itself have also surfaced. A recent case involving a Portuguese appellate court gave rise to public scrutiny following allegations that AI-generated content may have been used in judicial reasoning. Although the matter remains exceptional, it has triggered debate regarding transparency, accountability and the appropriate boundaries for AI-assisted decision-making in the judicial context.

This debate has been accompanied by the emergence of institutional guidance at both European and national levels.

At national level, the High Council for the Judiciary (*Conselho Superior da Magistratura*) has issued recommendations governing the use of AI in judicial activity. These confirm that AI systems may only be used as strictly auxiliary tools, such as for legal research or drafting, while preserving full judicial responsibility, prohibiting any substitution of human decision-making and requiring effective human control.

5. AI Regulatory Oversight

5.1 Regulatory Agencies

Portugal has adopted a decentralised supervisory model for AI oversight, aligned with Article 77 of the AI Act.

The Portuguese government has formally designated the national authorities responsible for supervising compliance with EU rules protecting fundamental rights in the context of high-risk AI systems. These include sectoral regulators, inspectorates and enforcement authorities across telecommunications, labour, healthcare, education, justice, defence, media, energy and consumer protection.

The Portuguese government has publicly announced its intention to designate ANACOM as the national point of contact under the AI Act. Once formally implemented, ANACOM is expected to assume a co-ordination role across the designated authorities and to support consistent supervisory practices in the application of the Regulation.

Other relevant regulators include:

- the Portuguese Data Protection Authority (CNPD);
- the Authority for Working Conditions (ACT);
- the Health Regulatory Authority (ERS);
- the Food and Economic Safety Authority (ASAE); and
- sectoral inspectorates across education, justice, defence and public administration.

This model reflects Portugal's preference for leveraging existing regulatory expertise rather than creating a standalone AI regulator.

5.2 Regulatory Directives

Portugal has not yet issued comprehensive AI-specific soft law by regulatory agencies. However, relevant interpretative guidance is emerging through sector-specific regulators and public institutions.

CNPD guidance on biometric data, employee monitoring, automated decision-making and international transfers remains directly relevant to AI deployments involving personal data.

The High Council for the Judiciary has issued recommendations on the use of AI in judicial activities, confirming that AI must remain strictly auxiliary and subject to full human oversight.

The former Administrative Modernisation Agency has also published GuIA, a practical framework for ethical, transparent and responsible AI in public administration.

As AI adoption increases, sectoral authorities are expected to issue additional interpretative guidance within their respective fields of competence.

5.3 Enforcement Actions

As of today, Portugal has not yet seen formal public enforcement proceedings specifically grounded on the AI Act.

Nevertheless, existing regulators have already been indirectly addressing AI-related risks through adjacent legal frameworks.

CNPD has adopted an increasingly interventionist position regarding biometric technologies, automated processing and facial recognition, including formal opinions concerning AI-assisted identification systems in public administration.

At consumer level, class actions against major digital platforms involving large-scale data processing, profiling and algorithmic decision-making are increasingly common, creating indirect judicial pressure on AI governance.

The absence of formal AI-specific enforcement should therefore not be interpreted as regulatory passivity. Rather, Portugal is moving towards a phased enforcement model built on existing regulators and sectoral expertise.

6. Standard-Setting Bodies

6.1 National Standard-Setting Bodies

Portugal does not currently have a dedicated national technical body focused exclusively on AI standardisation.

National implementation currently relies on alignment with European standardisation frameworks, particularly those developed by CEN, CENELEC and ETSI, which are expected to play a central role in supporting compliance with the AI Act.

At policy level, initiatives such as AI Portugal 2030, the National AI Agenda and public-sector guidance developed by the former Administrative Modernisation Agency provide operational governance frameworks, although not formal technical standards.

Portuguese companies operating in AI-intensive sectors are therefore expected to align with European harmonised standards as they emerge, particularly in areas such as risk management, conformity assessment, cybersecurity, transparency and human oversight.

6.2 International Standard-Setting Bodies

International standards are becoming increasingly relevant for organisations deploying AI in Portugal, particularly in anticipation of harmonised standards under the AI Act.

The most relevant frameworks currently include:

- ISO/IEC 42001, addressing AI management systems;
- ISO/IEC 23894, focused on AI risk management;
- ISO/IEC 22989, providing foundational AI concepts;
- relevant IEEE standards; and
- the NIST AI Risk Management Framework, particularly for multinational organisations operating across EU and US markets.

Although these standards are not legally binding, they are increasingly used as evidence of good governance, technical robustness and compliance readiness.

For Portuguese companies, adoption of internationally recognised standards may significantly facilitate future conformity assessments, procurement processes and cross-border commercial deployment.

7. AI and the State

7.1 Government Use of AI

Portugal has adopted a progressive approach to the use of AI in public administration, combining digital transformation policies, pilot deployments and ethical governance initiatives. The Strategy for the Digital Transformation of Public Administration 2021–2026 expressly promotes the use of data-driven technologies to improve public services, support administrative decision-making and enhance transparency.

In practice, public-sector deployments currently focus on conversational AI, natural language processing, knowledge retrieval and decision-support tools. Examples include the Sigma chatbot integrated into the ePortugal portal, the Virtual Assistant launched in 2023 using Azure OpenAI Service to support citizen interactions with digital public services, and the AI-powered Practical Guide to Justice launched in 2025 through a partnership involving the Ministry of Justice, Microsoft and Legislation Studio, designed to answer citizens' questions on family, civil and corporate matters.

At policy level, AI adoption is also reflected in the National Artificial Intelligence Agenda and in broader digital modernisation initiatives led by the former Agency for Administrative Modernisation (AMA).

From a legal and regulatory perspective, public bodies remain subject to the GDPR, constitutional principles such as equality, proportionality and good administration, and administrative-law requirements relating to transparency, reason-giving and human review of decisions affecting individuals. Where AI systems qualify as high-risk under the AI Act, public authorities must also comply with obligations relating to risk management, human oversight, documentation and fundamental rights protection.

7.2 Judicial Decisions

To date, no publicly reported judicial decisions in Portugal have directly addressed challenges to the use of artificial intelligence systems by public administration bodies. Similarly, no significant publicly known litigation has yet established judicial precedent regarding

administrative decisions materially supported or generated by AI systems.

The most visible AI-related judicial controversy to date involved a Portuguese appellate court, following public allegations that portions of a judicial decision may have been generated using generative AI tools. Although the matter did not concern the use of AI by government agencies, it prompted institutional scrutiny and broader public debate regarding judicial transparency, accountability and the permissible use of AI in adjudicative functions.

At institutional level, the High Council for the Judiciary subsequently issued guidance confirming that AI tools may only be used in a strictly auxiliary capacity, preserving full judicial independence, human responsibility and the prohibition of automated substitution of judicial reasoning.

7.3 National Security

The AI Act expressly excludes AI systems developed or used exclusively for military, defence or national security purposes. As a result, AI systems deployed in these contexts fall outside the AI Act's harmonised regulatory framework and remain primarily subject to national defence legislation, constitutional principles, export-control rules and applicable public international law, including international humanitarian law and human rights obligations.

In practice, Portuguese public-security authorities are already deploying AI-enabled tools in operational environments. The National Republican Guard (GNR), for example, uses artificial intelligence in geographic information systems and terrain-risk modelling to analyse patterns associated with criminal activity, support situational awareness and improve the proactive allocation of operational resources.

From publicly available information, the Ministry of National Defence and the Portuguese Armed Forces are also involved in innovation projects involving AI, although operational details remain limited for security reasons. Portugal additionally participates in European defence co-operation mechanisms, including PESCO and European Defence Fund initiatives, where AI applications are being explored in areas such as intelligence, surveillance, reconnaissance, cybersecurity and operational resilience.

Where AI technologies developed for civilian purposes may have dual-use applications, they remain subject to export-control obligations under Regulation (EU) 2021/821. Organisations developing advanced AI systems should therefore assess whether their technologies could fall within dual-use or defence-related regulatory frameworks.

8. Generative AI

8.1 Generative AI: Key Legal Issues and Regulatory Approaches

The legal framework for generative AI in Portugal is primarily shaped by the EU AI Act and by existing rules on data protection, consumer protection, intellectual property, confidentiality, cybersecurity, product safety and civil liability. The issues raised by generative AI are therefore dealt with through a combination of horizontal and sector-specific regimes, rather than through a separate national framework.

Generative AI is particularly challenging because it can produce text, images, code, audio, video and synthetic media at scale, often through foundation models whose training data and internal functioning are not fully transparent to users. Under the AI Act, providers of general-purpose AI models are subject to obligations on technical documentation, information to downstream providers, copyright-related policies and, for models with systemic risk, additional risk assessment and mitigation duties.

For organisations deploying generative AI in Portugal, the most relevant issues are practical. They should assess whether personal data is processed in prompts, uploaded documents, outputs, logs or model-improvement cycles; whether outputs may infringe third-party IP rights; whether users are informed that they are interacting with, or receiving, AI-generated content; and whether contractual terms allocate rights and liability clearly.

9. Legal Tech

9.1 AI in the Legal Profession and Ethical Considerations

Portuguese law firms are increasingly using AI tools for legal research, document review, due diligence, contract analysis, drafting support, translation, summarisation, billing, knowledge management and internal training. More recent use cases include generative AI tools and agentic workflows that assist lawyers in searching internal databases, comparing documents, preparing first drafts or organising large volumes of legal and evidentiary material.

The Portuguese Bar Association has not yet adopted binding AI-specific rules for legal practice. It has, however, actively promoted training, public debate and professional discussion regarding generative AI, large language models and AI agents. The applicable framework therefore continues to derive from the general professional regime governing lawyers, including duties of independence, competence, diligence, personal responsibility and professional secrecy.

In practice, AI must be treated as a strictly assistive tool rather than a substitute for legal judgement. Particular caution is required when using cloud-based general-purpose models, especially where prompts, uploaded documents, client communications or privileged materials could be retained, processed or reused for model-improvement purposes. Lawyers must also address risks associated with hallucinated authorities, fabricated case law, outdated sources, biased outputs and over-reliance on automated legal conclusions.

10. Liability for AI

10.1 General Theories of Liability

Portugal does not currently provide for a specific liability regime tailored to artificial intelligence. As such, liability continues to be assessed under general civil and contractual principles, typically requiring proof of an unlawful act or omission, fault (intent or negligence), damage and a causal link between conduct and harm.

In the context of AI systems, this framework raises practical difficulties. The autonomous or semi-autonomous behaviour of certain systems, combined with limited transparency and traceability, can make it challenging to identify the responsible party and establish causation. These features may, in practice, undermine the ability of claimants to meet the evidentiary threshold required under traditional fault-based regimes.

Existing product liability rules also remain relevant. The revised Product Liability Directive extends strict liability to defective digital products, expressly encompassing software and AI-enabled systems. This development is likely to play a central role in addressing AI-related harm, particularly where defects can be framed in terms of safety expectations or performance failures.

In parallel, market practice is increasingly relying on contractual allocation of risk across the AI value chain. Agreements between developers, deployers and users commonly include provisions addressing liability caps, indemnities, performance standards and compliance obligations, often supported by technical safeguards such as logging, traceability and audit mechanisms.

10.2 Regulatory Approaches to Liability for AI

At national level, there are no immediate legislative initiatives in Portugal aimed specifically at AI liability. The regulatory trajectory is instead being shaped at EU level, with member states expected to implement and operationalise forthcoming instruments.

In particular, the revised Product Liability Directive must be transposed by December 2026, introducing a modernised framework that explicitly captures digital products and AI systems. This will be complemented by the broader architecture established by the AI Act, including its enforcement and compliance mechanisms.

At policy level, the European approach has been moving towards facilitating claims by individuals affected by AI systems. This includes efforts to ease evidentiary burdens, improve access to relevant information and mitigate the “black box” problem, thereby enhancing the effectiveness of existing liability frameworks.

Despite these developments, key challenges remain, particularly in relation to the assessment of defectiveness, the attribution of fault and the disclosure of technical evidence. Addressing these issues will require not only legislative refinement but also technical and operational solutions, including improved documentation, explainability and traceability of AI systems.

11. Agentic AI Systems and Autonomous Decision-Making

11.1 Agentic AI Systems: Legal Framework and Governance

Portuguese law does not currently treat agentic AI systems as a distinct legal category. Their assessment therefore depends on the applicable general framework, including the EU AI Act, the GDPR, contract law, civil liability, consumer protection, cybersecurity rules and sector-specific regulation.

The relevant legal question is less whether a system is described as "agentic" in the abstract, and more what the system is designed and permitted to do. Agentic AI systems typically combine a language model with instructions, memory, planning capabilities and tools that allow interaction with external systems. Depending on their architecture, they may search databases, generate documents, update records, trigger workflows, make recommendations or interact with other agents. The system's risk profile will therefore depend on its access to data and tools, the reversibility of its actions, the sensitivity of the context and the level of human supervision.

The use of agentic AI does not, in itself, displace accountability from the persons or organisations involved in its development, deployment or use.

Governance should therefore be defined before deployment, including the agent's permitted scope of action, access permissions, approval workflows, escalation rules, technical safeguards and conditions for human intervention. Where multiple organisations or interoperable agents are involved, contractual arrangements should also clearly allocate responsibilities relating to data access, instructions, supervision, incident response and remediation.

Auditability remains a central requirement. Organisations should maintain logs capable of reconstructing the agent's instructions, inputs, outputs, tool usage, interactions with third-party systems, overrides and decision pathways, particularly where the agent may materially affect individuals, customers, assets or regulated operations.

11.2 Liability Allocation for Autonomous AI Systems

There is no AI-specific Portuguese liability regime for autonomous or agentic AI systems. General contractual and non-contractual liability rules apply, together with product liability, consumer protection and sector-specific regimes where relevant. The main difficulty is practical and evidentiary: harm may result not from a single act, but from a combination of model design, system integration, deployment choices, user instructions, excessive permissions, insufficient oversight and autonomous execution.

Developers and providers may be exposed where harm results from defective design, inadequate documentation, misleading claims, insufficient safeguards or failure to comply with applicable AI Act obligations. Deployers may be liable where the system is used outside its intended purpose, connected to unnecessary databases or tools, deployed without appropriate oversight, or operated in disregard of foreseeable risks. Users may also be relevant where they misuse the system or intentionally bypass safeguards.

Contractual allocation is therefore particularly important. Agreements should address permitted use, performance limits, access to tools and data, compliance warranties, security, audit rights, incident notification, human oversight, responsibility for outputs, indemnities and liability caps. In multi-agent environments, contracts should also cover dependencies on third-party tools, agent-to-agent interactions and cascading failures. Reliable logging of instructions, tool calls, data accessed, outputs, actions, approvals and overrides will be essential to establish causation, fault and accountability.

12. Specific Legal Issues With AI

12.1 Algorithmic Bias and Fairness

In Portugal, algorithmic bias is primarily addressed through the combined application of the AI Act, the GDPR, constitutional equality principles, anti-discrimination legislation, labour law and sector-specific regulation, rather than through a dedicated national statute.

From a technical perspective, bias may arise from multiple sources, including unrepresentative training data, historical or societal imbalances, proxy variables, labelling errors, feedback loops or model optimisation choices that systematically disadvantage certain groups.

From a legal perspective, discriminatory outcomes generated or supported by AI systems may engage constitutional protections, anti-discrimination rules, employment law, consumer protection and data protection obligations. Article 13 of the Portuguese Constitution enshrines the principle of equality, while existing sectoral frameworks prohibit discriminatory treatment on grounds such as sex, race, ethnic origin, religion, disability, age, sexual orientation or political opinion.

Within the EU framework, the AI Act addresses algorithmic bias primarily through its requirements for high-risk systems, including risk management, data governance, technical documentation, human oversight, accuracy, robustness and conformity assessment. In particular, Article 10 requires providers to implement data governance measures designed to identify and mitigate relevant biases throughout development, validation and testing.

Where required under the AI Act, deployers of certain high-risk systems must also perform fundamental rights impact assessments before operational use, particularly where decisions may materially affect individuals.

Liability for discriminatory outcomes may arise under contractual, tort, employment, consumer-protection or regulatory frameworks, depending on the context of deployment and the degree of human oversight retained.

12.2 Biometric Technologies and Emotion Recognition

The AI Act, with its prohibitions on certain AI practices applicable since 2 February 2025, prohibits, among other uses, real-time remote biometric identification systems in publicly accessible spaces for law-enforcement purposes, subject to narrowly defined exceptions; AI systems used to infer emotions in workplaces and educational institutions, except where justified by medical or safety considerations; and biometric categorisation systems based on sensitive attributes.

Under Article 9 of the GDPR, facial recognition and biometric data are classified as special categories of personal data, the processing of which is generally prohibited unless a specific legal basis applies. At national level, Law No. 58/2019 expressly limits the use of biometric data in employment relationships to attendance-recording and access-control purposes.

The Portuguese Data Protection Authority (CNPD) has consistently adopted a restrictive approach to biometric surveillance and large-scale monitoring. In Opinion No 2021/143, the CNPD expressed significant concerns regarding the use of video-surveillance images, drones, AI-enabled monitoring tools, biometric capture and the broader deployment of camera-based technologies in public spaces, including in public-safety contexts.

Although biometric identifiers may be used in criminal investigation under specific legal frameworks (eg, fingerprints), no publicly known operational programmes involving live facial-recognition surveillance have been deployed in Portugal to date.

12.3 Deepfakes and Synthetic Media

The AI Act imposes specific transparency obligations in relation to deepfakes and synthetic media. Under Article 50 (4), persons deploying AI systems that generate or manipulate image, audio or video content constituting deepfakes must clearly disclose that such content has been artificially generated or manipulated. Similar transparency obligations may also apply to synthetic text made available to the public on mat-

ters of public interest, subject to important journalistic, editorial and lawful-expression exceptions.

At platform level, the Digital Services Act, implemented into national law by Law No 12-A/2026, of 15 April, imposes due-diligence obligations on online intermediaries regarding illegal content, including deepfakes used for fraud, identity theft, defamation, market manipulation or non-consensual intimate imagery. Depending on their size and risk profile, platforms may be required to implement notice-and-action mechanisms, content-moderation procedures and systemic-risk mitigation measures.

Under Portuguese law, victims of harmful deepfakes may rely on general civil liability principles, personality rights protected under Articles 70 to 81 of the Civil Code, image rights, privacy protections and, where applicable, consumer protection rules. Available remedies include injunctive relief, takedown requests, reputational remediation and compensation for patrimonial or non-patrimonial harm.

Malicious uses of synthetic media may also trigger criminal liability under rules relating to fraud, identity misuse, defamation, computer crime, sexual offences or unlawful disclosure of intimate content.

From a technical-governance perspective, organisations increasingly rely on provenance metadata, watermarking, content credentials, forensic detection tools and internal verification workflows to authenticate digital content and reduce manipulation risks.

Sector-specific restrictions may become particularly relevant in areas such as journalism, elections, financial services, public communications and online advertising, where synthetic media may affect market integrity, democratic processes or public trust.

12.4 Transparency and Disclosure

The AI Act introduces a risk-based transparency framework, imposing disclosure, documentation and traceability obligations depending on the type of system, its intended use and the risks involved. Transparency under the AI Act does not require universal disclosure of all AI use, but instead focuses on specific use cases where individuals, deployers or regulators need sufficient information to understand that AI is being used, assess outputs appropriately and exercise legal rights.

Under Article 50 (1), persons deploying AI systems intended to interact directly with natural persons, including chatbots and virtual assistants, must clearly inform users that they are interacting with an AI system, unless this is obvious from the context.

The AI Act also imposes specific transparency obligations for synthetic content. Deepfakes and certain AI-generated content made available to the public must be clearly disclosed as artificially generated or manipulated, using appropriate machine-readable markings, provenance metadata or equivalent technical measures, subject to exceptions for authorised law-enforcement activities and certain journalistic, artistic, satirical or editorial contexts.

High-risk AI systems must comply with Article 13 and related documentation obligations, ensuring sufficient transparency, interpretability and traceability to enable deployers to understand system capabilities, limitations and outputs, and to exercise meaningful human oversight.

Under the GDPR, individuals retain rights relating to automated decision-making, including information about the existence of automated processing and, where applicable, meaningful information about the logic involved.

Providers of general-purpose AI models must also make available technical documentation, information on training methodologies, model capabilities, limitations and copyright-compliance measures to downstream providers and deployers. Models presenting systemic risk are subject to enhanced transparency, testing, cybersecurity and incident-reporting obligations.

The AI Act additionally prohibits manipulative AI practices involving subliminal techniques or exploitation of vulnerabilities where such practices materially distort behaviour and cause or are likely to cause significant harm.

13. AI Procurement and Supply Chain Accountability

13.1 AI Procurement Standards and Contracting

AI procurement in Portugal is increasingly treated as a governance and risk-allocation exercise rather than a conventional software acquisition. While existing procurement principles remain broadly applicable, the acquisition of generative, predictive or agentic AI systems introduces additional contractual, operational and regulatory complexities, particularly where systems continuously learn, interact with third-party tools, access sensitive datasets or influence business-critical decisions.

In practice, negotiations increasingly concentrate around a limited number of recurring issues. These include restrictions on provider use of prompts, inputs, outputs and telemetry data for model improvement; ownership and permitted use of fine-tuned models, embeddings, model outputs and derivative assets; compliance with the AI Act, the GDPR, cybersecurity obligations and sector-specific regulation; and the allocation of responsibility for inaccurate, infringing, biased, hallucinated or operationally harmful outputs.

Service level agreements should go beyond traditional uptime metrics and address response times, inference latency, accuracy thresholds, availability of human escalation, model-version changes, incident response and continuity of critical functionality. Where agentic systems are involved, contracts should also address tool-calling permissions, autonomous execution thresholds, third-party API dependencies and approval workflows for high-impact actions.

Audit rights, access to technical documentation, logging records, model-performance data and compliance evidence are increasingly treated as essential. Exit strategy, portability, and concentration risks associated with hyperscaler infrastructure or proprietary model ecosystems should also be addressed.

13.2 AI Supply Chain Accountability and Due Diligence

The AI Act adopts a value-chain approach to AI governance, allocating differentiated obligations across providers, deployers, importers, distributors, authorised representatives and, in certain circumstances, entities substantially modifying existing systems. As a result, compliance increasingly depends not only on the characteristics of the AI system itself, but also on the integrity, transparency and accountability of the broader technical and contractual ecosystem in which that system operates.

In practice, organisations procuring high-risk AI systems in Portugal should conduct structured due diligence before deployment, including verification of CE marking, conformity-assessment status, technical documentation, intended purpose, known limitations, data-governance measures, cybersecurity safeguards and the provider's ability to support ongoing regulatory compliance.

Where AI systems rely on upstream third-party components – such as pre-trained models, foundation models, APIs, datasets, cloud infrastructure or open-source modules – organisations should assess the provenance, licensing terms, security posture, performance limitations and compliance posture of those dependencies. While obligations under the AI Act remain role-specific, deployers may still face operational, contractual or regulatory exposure where third-party components materially affect system behaviour, safety or compliance.

The AI Act also imposes extensive documentation and traceability obligations across the value chain, including technical documentation, logging, instructions for use, post-market monitoring and, where applicable, registration in the EU database. These requirements are designed to support provenance, auditability, incident investigation and regulatory supervision.

14. Employment

14.1 Hiring and Termination Practices

Portuguese law does not expressly prohibit the use of AI tools in recruitment or termination processes. However, their deployment is subject to a robust labour law framework, particularly in relation to equality, non-discrimination and procedural fairness.

To mitigate the risk of discriminatory practices, the Portuguese Labour Code requires employers to maintain detailed records of recruitment procedures, including information on applications, selection stages and outcomes, typically disaggregated by gender. These obligations aim to ensure transparency and enable scrutiny of potential biases, whether human or algorithmic.

The use of AI-driven tools in hiring must therefore be carefully calibrated to avoid indirect discrimination, particularly where automated decision-making may replicate or amplify existing biases embedded in training data.

Termination practices remain subject to strict legal constraints. Dismissal without cause is not permitted, and employers must provide duly substantiated written grounds. In addition, specific protective regimes apply in certain circumstances, including for pregnant employees, employees exercising parental rights or informal carers, where notification obligations towards the competent authority are triggered.

In this context, while AI may support decision-making processes, it cannot replace the legal requirement for human accountability and justification, particularly in matters affecting job security.

14.2 Employee Evaluation and Monitoring

The use of AI in employee monitoring is subject to significant legal limitations under Portuguese law.

As a general rule, the Portuguese Labour Code prohibits the use of remote surveillance technologies for the purpose of monitoring employee performance. Electronic monitoring is only permitted where it is necessary for the protection of persons and property or justified by the specific nature of the activity carried out.

The CNPD has reinforced this restrictive approach through guidance that effectively prohibits systematic monitoring of employees. This includes, in particular, tools capable of tracking browsing activity, recording keystrokes or mouse movements, capturing screen content, monitoring application usage or analysing time spent on specific tasks.

Data collected through surveillance systems may only be used in disciplinary proceedings where it reveals conduct that may constitute a criminal offence, and insofar as it is processed within the context of criminal proceedings, significantly limiting its practical utility for performance management purposes.

Biometric data may be processed, but only for limited purposes such as access control and attendance recording, and remains subject to strict proportionality requirements. In addition, its use typically requires a prior data protection impact assessment, given the heightened risks associated with this category of data.

15. AI in Industry Sectors

15.1 Digital Platform Companies

Digital platform companies are among the most intensive users of artificial intelligence in Portugal, deploying AI across recommender systems, content moderation, targeted advertising, fraud detection, dynamic pricing, logistics optimisation, customer support and the matching of users, sellers, drivers or service providers. Practical examples include algorithmic management systems used by Uber and Glovo in ride allocation, route optimisation, dynamic pricing and fraud detection, as well as recommendation, ranking and personalisation systems used by platforms such as Amazon and Booking.com in e-commerce and hospitality services.

Although these systems are not regulated as a distinct category under Portuguese law, their deployment is subject to an increasingly dense combination of EU and national regulatory frameworks. The most relevant legal regimes include the AI Act, the GDPR, consumer protection rules, e-commerce legislation, the Digital Services Act and, where relevant, competition, employment and sector-specific regulation.

In practice, platform operators should pay particular attention to profiling, automated decision-making, transparency of ranking and recommendation systems, dark patterns, personalised pricing, discriminatory outcomes, synthetic or AI-generated content, chatbot disclosures and the use of generative AI in consumer-facing interactions. Where platforms use AI

to allocate tasks, monitor performance, rank service providers, adjust remuneration or suspend accounts, labour law, platform work and anti-discrimination considerations may also become relevant.

From an enforcement perspective, AI-enabled platform practices may attract scrutiny from CNPD in matters involving profiling and behavioural analytics, from *Autoridade de Segurança Alimentar e Económica* (ASAE) in relation to misleading commercial practices and dark patterns, and from *Autoridade da Concorrência* (the Portuguese Competition Authority) where algorithmic pricing, ranking or self-preferencing materially affect market dynamics.

15.2 Financial Services

Artificial intelligence is increasingly used across the Portuguese financial sector in areas such as fraud detection, AML/CFT transaction monitoring, sanctions screening, payment verification, creditworthiness assessments, robo-advice, customer support, claims handling, portfolio optimisation, market surveillance and algorithmic trading. These applications can materially improve operational efficiency, personalisation and risk detection, but they also raise legal and supervisory concerns relating to explainability, discrimination, model risk, cybersecurity, outsourcing and over-reliance on automated outputs.

Financial institutions operating in Portugal must assess AI deployments against a combination of the AI Act, the GDPR, financial-services regulation, anti-money laundering rules and sector-specific supervisory expectations. Credit scoring, underwriting and creditworthiness assessments are particularly sensitive, as they may qualify as high-risk under the AI Act and may also trigger GDPR restrictions relating to profiling and automated decision-making producing legal or similarly significant effects.

At national level, AI deployments may attract scrutiny from *Banco de Portugal*, *Comissão do Mercado de Valores Mobiliários* and *Autoridade de Supervisão de Seguros e Fundos de Pensões*, particularly in areas involving consumer protection, prudential risk, outsourcing, operational resilience and model governance.

Since the entry into application of the Digital Operational Resilience Act (DORA), financial entities must also ensure that AI systems and related ICT providers are incorporated into ICT-risk frameworks, third-party risk management, incident reporting, resilience testing, change-management processes and board-level governance structures.

15.3 Healthcare

Artificial intelligence is increasingly being deployed in the Portuguese healthcare sector in areas such as clinical decision support, medical imaging, radiology, dermatology, triage, patient monitoring, administrative prioritisation, drug discovery, research analytics and operational resource planning. Public and private healthcare providers, including entities operating within the *Serviço Nacional de Saúde* ecosystem, are progressively exploring AI-enabled tools to improve diagnostic efficiency, optimise patient pathways and support data-driven clinical decision-making.

Because these systems frequently involve health data, vulnerable individuals and decisions affecting diagnosis, treatment or access to care, they operate within a particularly demanding legal environment. Health data qualifies as a special category of personal data under the GDPR, and AI deployments may also trigger obligations under the AI Act, medical-device regulation, product-safety legislation, cybersecurity rules and professional-liability frameworks.

Where AI systems perform diagnostic, therapeutic or clinical decision-support functions, they may qualify as software-based medical devices under the EU Medical Devices Regulation and, in many cases, as high-risk systems under the AI Act. As a result, providers and healthcare institutions must address clinical validation, human oversight, explainability, post-market monitoring, incident reporting and cybersecurity controls.

At national level, AI deployments may attract scrutiny from INFARMED in relation to medical-device compliance, from *Entidade Reguladora da Saúde* in relation to patient safety and quality-of-care obligations, and from CNPD in matters involving health-data processing, secondary use of datasets or automated decision-making.

15.4 Autonomous Vehicles

Portugal has recently moved towards a specific framework for autonomous vehicle testing. In April 2026, the government announced the approval of a decree-law establishing a dedicated legal regime for the public-road testing of autonomous driving and connected mobility systems. According to the government's announcement, the regime is focused on testing and validation rather than general commercial deployment, and requires prior authorisation from the Institute for Mobility and Transport (IMT), together with strict requirements relating to vehicles, drivers and operators, mandatory safety and cybersecurity plans, reinforced civil liability insurance and continuous data-recording systems for evidentiary purposes.

15.5 Retail and Consumer

Retail and consumer-facing businesses are increasingly using artificial intelligence in Portugal across personalised recommendations, customer segmentation, dynamic pricing, stock optimisation, demand forecasting, fraud detection, conversational commerce, virtual assistants, automated product descriptions, image generation, targeted advertising and after-sales support. Generative AI is also increasingly used in marketing campaigns, customer engagement, content localisation and internal content production.

The main legal risks concern transparency, fairness, profiling and consumer trust. Businesses deploying AI in consumer-facing environments should ensure that consumers are not misled regarding AI-generated content, personalised recommendations, chatbot interactions, synthetic product imagery, promotional claims or algorithmically personalised pricing. Particular attention should also be given to dark patterns, behavioural manipulation and the use of AI techniques capable of materially influencing consumer decision-making.

From a regulatory perspective, the most relevant frameworks include the AI Act, the GDPR, ePrivacy rules, consumer-protection legislation, advertising rules, e-commerce law and, where relevant, competition law. AI systems relying on cookies, loyalty programmes, behavioural analytics, purchase histories or location data may also trigger obligations relating to profiling, consent, transparency and automated decision-making.

From an enforcement perspective, AI-enabled retail practices may attract scrutiny from ASAE in matters involving unfair commercial practices, misleading advertising or dark patterns, from CNPD where profiling or behavioural analytics involve personal data, and from *Autoridade da Concorrência* where algorithmic pricing, self-preferencing or data-driven market strategies materially affect competition.

15.6 Industrial AI and Robotics

Industrial AI is used in Portugal for predictive maintenance, quality control, production optimisation, logistics, robotics, digital twins, energy management and supply-chain forecasting. These systems may not always interact directly with individuals, but they can have significant operational, safety, cybersecurity and liability implications, particularly where they are embedded in production lines, machinery, autonomous systems or safety-critical processes.

The applicable framework depends on the function, sector and risk profile of the system. Where AI is embedded in machinery, robotics, safety components or industrial control systems, the AI Act, EU product safety and product liability rules, sector-specific safety legislation and the forthcoming full application of the EU Machinery Regulation will be particularly relevant. In industrial environments, liability may arise from defective products, workplace accidents, failures in maintenance, insufficient human oversight, cybersecurity incidents or incorrect operational decisions affecting production, equipment or personnel.

Companies should therefore focus on technical documentation, conformity assessment, testing, validation, post-market monitoring, cybersecurity, human oversight, incident response and clear contractual allocation of responsibility between manufacturers, integrators, software providers, maintenance providers and operators. For entities operating in essential or important sectors, cybersecurity governance and incident-reporting obligations under the Portuguese NIS2 transposition may also need to be considered.

16. Intellectual Property

16.1 IP Protection for AI Assets

AI systems and their components are protected under existing EU and Portuguese intellectual property frameworks, although these regimes do not specifically address AI technologies. The National Artificial Intelligence Agenda also anticipates a review of the IP and patent framework for AI, with a view to providing clearer standards for research institutions and businesses.

Patent protection may be available for AI-related inventions where they produce a demonstrable technical effect beyond abstract computational methods. However, purely algorithmic innovations or data-driven models without a technical contribution are generally excluded.

Copyright protection applies to software code, model architectures (where sufficiently original) and certain datasets. Database rights may also protect structured datasets where there has been substantial investment in obtaining, verifying or presenting the data.

Trade secrets are particularly relevant for AI assets, including model weights, training methodologies, data pipelines and optimisation techniques. In many cases, trade secret protection offers more practical value than formal IP rights, particularly given the difficulty of meeting patentability thresholds.

Contractual arrangements play a central role in allocating IP rights, particularly in collaborative development, licensing and use of third-party models. Terms imposed by AI providers – especially for general-purpose AI systems – can significantly affect ownership, permitted uses and downstream exploitation of both inputs and outputs, including through restrictions on training, reuse and commercial deployment.

16.2 AI as Inventor/Author

Under current Portuguese, EU and international intellectual property frameworks, AI systems cannot be recognised as inventors or authors for the purposes of patent or copyright protection. Inventorship and authorship remain legally linked to natural persons, reflecting the fundamentally anthropocentric structure of existing intellectual property regimes. This position has been consistently upheld by patent offices and courts in multiple jurisdictions, including in the well-known DABUS decisions before the European Patent Office, the UK Intellectual Property Office, the United States Patent and Trademark Office and other national authorities, all of which rejected the designation of an AI system as inventor.

Under Portuguese law, there is currently no statutory basis for recognising an AI system as an inventor or author. Patent applications must identify a human inventor, and copyright protection presupposes an original intellectual creation attributable to a natural person. Accordingly, purely autonomous machine-generated inventions or creative outputs, without sufficient human intellectual contribution, may face uncertainty regarding the availability of formal IP protection.

In practice, ownership of AI-assisted inventions or works is generally attributed to the individual or individuals who made the relevant inventive or creative contribution, or to their employer or commissioning entity where applicable under employment, contractual or corporate ownership rules. The key legal question is therefore not whether AI participated in the creation process, but whether there was sufficient human involvement in defining objectives, selecting data, designing methodologies, curating outputs, exercising creative judgment or otherwise shaping the final result.

This creates increasing legal complexity where AI systems operate with a high degree of autonomy, particularly in areas such as generative design, autonomous optimisation, scientific discovery and creative content generation, where the boundary between human contribution and machine-generated output may become difficult to establish.

Moral rights considerations may also arise, particularly under Portuguese copyright law, where rights of attribution, integrity and author identification are inherently personal and can only vest in human authors. Where content is substantially generated by AI, questions may arise as to whether any person can legitimately claim authorship, how attribution should be

presented and whether modifications of AI-assisted works engage moral rights protections.

16.3 Copyright and AI Training Data

The use of copyrighted works for AI training remains one of the most contested legal issues in the AI ecosystem and is currently the subject of significant regulatory, judicial and commercial debate in Europe and internationally. In Portugal, as in other EU Member States, the legal analysis is primarily shaped by copyright law, database rights, trade secret protections, contractual restrictions and the text and data mining (TDM) framework established under Directive (EU) 2019/790 on copyright in the Digital Single Market, as implemented into national law by Decree-Law No 47/2023.

Under the EU TDM framework, certain reproductions and extractions of protected works may be permitted for training purposes without prior authorisation. Article 3 establishes a mandatory exception for research organisations and cultural heritage institutions carrying out scientific research, subject to lawful access requirements. Article 4 provides a broader exception that may apply to commercial operators, including AI developers, provided that rights holders have not expressly reserved their rights through machine-readable or other appropriate opt-out mechanisms.

Where protected works, databases, software, audiovisual content, images, text or other copyright-protected materials are used for training without a valid exception, licence or other lawful basis, copyright infringement claims may arise depending on the nature of the copying, extraction, storage, transformation and model training process. Separate issues may also arise under database rights, contractual access restrictions, website terms of use, technological protection measures and confidentiality obligations.

Licensing frameworks are emerging as a practical commercial response, including collective licensing initiatives, direct licensing arrangements, dataset marketplaces and sector-specific content partnerships. However, these frameworks remain fragmented, jurisdictionally inconsistent and commercially immature, particularly in relation to large-scale general-purpose AI training.

Liability may also arise at the output stage where generated content reproduces, memorises, reconstructs or closely resembles protected works, software code, images, music, literary content or other identifiable expression contained in training datasets. The degree of similarity, the presence of substantial reproduction, the extent of memorisation and the level of human intervention may all become relevant factors in infringement analysis.

Ongoing litigation, particularly in the United States and the United Kingdom, is expected to shape key aspects of this debate, including the application of fair use, the distinction between transformative and reproductive uses, the legal relevance of model memorisation, and the evidentiary standards for establishing copying or substantial similarity. Similar debates are increasingly emerging before European regulators, courts and copyright stakeholders.

Issues of attribution, integrity and moral rights may also arise, particularly in civil law jurisdictions such as Portugal, where authors retain strong personal rights in relation to the attribution and integrity of their works. These issues may become particularly sensitive where AI-generated outputs imitate identifiable authors, artistic styles or culturally significant works.

At the regulatory level, the European Union AI framework does not currently create a new copyright regime, but the transparency obligations applicable to certain general-purpose AI providers, including obligations relating to training data summaries under the AI Act, are expected to increase scrutiny over the provenance, legality and governance of copyrighted training materials.

16.4 AI-Generated Works of Art and Works of Authorship

Under current Portuguese and EU copyright law, AI-generated works do not automatically qualify for copyright protection. Copyright protection remains dependent on the existence of an original intellectual creation attributable to a natural person, meaning that purely autonomous outputs generated by AI systems, without sufficient human creative contribution, may fall outside the scope of protection.

Where AI is used as an assistive or creative tool and there is meaningful human involvement in shaping the final output, such as through the selection of inputs, creative direction, iterative prompting, curation, editing, arrangement or other forms of intellectual intervention, copyright protection may still arise. In such cases, authorship is generally attributed to the human contributor or, where applicable, to their employer or commissioning entity under applicable employment, contractual or corporate ownership rules.

Moral rights considerations may also be relevant, particularly under Portuguese copyright law, where rights of attribution, integrity and author identification are personal rights that can only vest in human authors. Questions may therefore arise as to whether AI-assisted works can legitimately be attributed to a particular individual, whether subsequent modifications affect the integrity of the work, and how attribution should be presented in hybrid human-machine creative processes.

16.5 Foundation Models and Open-Source AI: IP Considerations

Foundation models raise complex intellectual property issues, particularly in relation to licensing, access, control, modification and downstream commercial exploitation.

Different licensing models currently coexist, including proprietary systems, open-weight models and open-source frameworks, each with distinct legal and commercial implications. Proprietary models typically provide access through contractual arrangements with limited rights of inspection or modification, while open-weight and open-source models may allow broader access to model parameters, source code or technical documentation, subject to applicable licence conditions.

The choice between API-based access and self-hosted deployment may also affect intellectual property rights, data governance and operational control. API-based models generally subject users to provider terms governing ownership of inputs and outputs, permitted uses, retention of submitted data, benchmarking, fine-tuning and commercial deployment. Self-hosted models may provide greater technical autonomy, but typically transfer greater responsibility for licence compliance, security, governance and infringement risk to the deployer.

Fine-tuning, parameter adaptation, transfer learning and other forms of model customisation may raise questions regarding derivative works, ownership of improvements and rights to commercialise adapted models. The legal position will often depend on the original licensing terms, the degree of technical modification and whether protected elements of the underlying model are reproduced or incorporated into the resulting system.

Open-source AI licences continue to evolve, including both traditional open-source software licences and AI-specific licensing frameworks imposing restrictions on redistribution, field of use, attribution, safety compliance or commercial exploitation. Although such licences are generally capable of contractual enforcement, their application in multi-layered AI supply chains involving datasets, model weights, inference services and downstream applications remains largely untested.

Commercial use of foundation models may also create intellectual property exposure where the provenance of training data is unclear, outputs reproduce protected content, embedded open-source components are not properly identified, or licensing obligations are incompatible with the intended business model.

Compliance with provider terms is therefore critical, particularly where providers restrict reverse engineering, model extraction, benchmarking, fine-tuning, commercial resale, regulated-sector deployment or the use of outputs for further model training.

17. Data Protection

17.1 AI Training and Data Protection

AI training is subject to the general Portuguese and EU data protection framework, rather than to a separate national regime. As a result, the relevant framework remains the GDPR, the Portuguese GDPR Implementation Law (Law No 58/2019, of 8 August) and, where

applicable, ePrivacy rules, complemented by the EU AI Act where the relevant system falls within its scope.

Where training datasets include personal data, organisations must identify an appropriate lawful basis under Article 6 GDPR. Consent may be suitable in controlled and clearly defined environments, but it will often be difficult to rely on for large-scale model training, particularly where data is obtained indirectly or collected from publicly available sources. Legitimate interests may be relevant in certain cases, including product improvement, fraud prevention, cybersecurity or internal analytics, but it requires a case-by-case assessment of necessity, proportionality, reasonable expectations and safeguards. Scientific research may also be relevant where the relevant GDPR conditions and safeguards are met.

Purpose limitation is one of the central challenges. Data collected for customer support, recruitment, healthcare, financial services, marketing or platform use cannot automatically be repurposed for training. Public availability of data does not, in itself, make that data freely usable for AI development. Organisations should therefore assess compatibility with the original purpose and ensure that the data used is adequate, relevant and limited to what is necessary.

Special category data, including health or biometric data, requires both an Article 6 lawful basis and an Article 9 condition. Pseudonymisation remains useful but does not take the data outside the GDPR. Anonymisation must be robust, particularly given risks of extraction, memorisation or regurgitation. Organisations should document dataset provenance, lawful basis, compatibility assessments, minimisation choices, retention, safeguards and residual risks.

17.2 AI Deployment and Data Subject Rights

The deployment of AI systems raises a separate set of data protection questions from those arising at the training stage. Even where a model was not trained on personal data, its use may involve the processing of prompts, uploaded documents, images, voice recordings, user logs, outputs, feedback data or customer and employee records.

The lawful basis will depend on the use case. Contractual necessity may apply where the AI functionality is genuinely required to provide the requested service. Legitimate interests may support internal productivity tools, customer support, fraud prevention or cybersecurity, provided the relevant balancing test is carried out. Consent may be required for optional features, marketing-related profiling or contexts where user choice is essential.

Transparency is a key requirement. Privacy notices should explain, in clear terms, when AI is used, what data is processed, for which purposes, on which lawful basis, whether data is used for model improvement, who receives it, how long it is retained and what rights are available. Generic references to “automation” or “technology” are unlikely to be sufficient where AI materially affects individuals.

Data subjects may exercise the usual GDPR rights, including access, rectification, erasure, restriction, portability and objection. Article 22 GDPR remains particularly relevant where AI is used for solely automated decisions producing legal or similarly significant effects, such as recruitment filtering, credit scoring, fraud blocking, insurance pricing or access to essential services.

Children’s data requires enhanced protection, including age-appropriate transparency, stricter default settings and careful consideration of profiling, persuasive design and long-term data use.

17.3 AI Data Governance and Cross-Border Transfers

A DPIA will often be required for AI systems, especially where processing involves large-scale profiling, special category data, vulnerable individuals, systematic monitoring, biometric technologies, employment decisions, credit scoring or other decisions with significant effects.

On 10 March 2026, the EDPB adopted a common DPIA template and accompanying explainer, aimed at helping controllers structure, harmonise and evidence DPIA reporting across the EU. The template was subsequently published for public consultation, and although its use is not yet mandatory, it is likely to

become an important reference point for supervisory authorities, either as a standalone template or as a "meta-template" for national approaches. This is particularly relevant for AI systems, where DPIAs should address data provenance, lawful basis, purpose compatibility, minimisation, bias and discrimination risks, security, explainability, human oversight, data subject rights, vendor dependencies, international transfers and the interaction between GDPR accountability and AI Act documentation.

18. Antitrust

18.1 Emerging Antitrust Issues in AI

AI is increasingly relevant to competition law in Portugal, both as a tool used by undertakings in downstream markets and as a market in itself. The main concerns are not limited to algorithmic collusion or AI-enabled pricing. They also include access to the inputs required to develop and deploy AI systems, such as data, cloud infrastructure, computing power, specialised chips, foundation models and distribution channels.

The Portuguese Competition Authority has been attentive to digital markets and has more recently addressed risks in the AI value chain. In February 2026, it published a short paper on competition issues associated with access to AI chips, noting that chips and related hardware, including through cloud computing services, are a determining input for the development of AI systems and that parts of the global value chain show high levels of concentration.

In practice, competition issues may arise from mergers and "acqui-hires", exclusive access to datasets or computing capacity, self-preferencing, tying or bundling of AI services with cloud or platform products, restrictions on interoperability, and vertical integration across foundation models, infrastructure and applications. AI systems may also facilitate collusion where competitors use pricing algorithms that monitor, react to or stabilise market behaviour.

19. Cybersecurity

19.1 Applicability of Cybersecurity Legislation to AI

Portugal's cybersecurity framework has become materially more relevant for organisations developing, procuring or deploying AI systems, particularly where those systems are embedded in critical digital infrastructure, essential services, connected products or high-impact operational environments.

At national level, the transposition of the NIS2 Directive through Decree-Law No 125/2025 significantly strengthens cybersecurity obligations for entities classified as essential or important, including in sectors such as digital infrastructure, energy, transportation, healthcare and space. The regime introduces governance, technical, organisational and supply chain security obligations, while also imposing direct accountability on management bodies for the approval and oversight of cybersecurity risk management measures.

Where AI systems are deployed within entities falling within the scope of this regime, cybersecurity obligations may extend well beyond traditional IT security. Organisations should assess risks associated with adversarial attacks, model manipulation, prompt injection, data poisoning, model extraction, unauthorised access to training environments, third-party APIs and dependencies on cloud or foundation model providers.

The AI Act reinforces this framework by requiring high-risk AI systems to achieve appropriate levels of accuracy, robustness and cybersecurity throughout their life cycle. Depending on the architecture involved, this may require secure development practices, access controls, logging, vulnerability management, testing against adversarial scenarios and technical safeguards designed to preserve integrity, availability and resilience.

Incident reporting may also be triggered under multiple regimes. Entities subject to the Portuguese NIS2 framework must comply with strict notification timelines in the event of significant cybersecurity incidents, while AI providers may also face additional obligations

under the AI Act depending on system classification and impact.

20. ESG

20.1 ESG Dimensions of AI

AI has an increasing ESG dimension for companies operating in Portugal. From an environmental perspective, the main concerns relate to energy consumption, data-centre capacity, cloud infrastructure, hardware supply chains and, for larger models, the carbon footprint associated with training and deployment. These issues may become relevant for companies subject to sustainability reporting where AI-related impacts, risks or dependencies are material.

The social dimension is equally important. AI systems may affect individuals through profiling, automated decision-making, algorithmic bias, workplace monitoring, access to services and the displacement or transformation of work. Companies should therefore assess whether AI use may create discriminatory outcomes, affect vulnerable groups or undermine transparency and human oversight.

From a governance perspective, AI should be integrated into existing compliance, risk and ESG structures rather than treated as a purely technical matter. This includes internal AI policies, clear allocation of responsibility, procurement due diligence, documentation, impact assessments, incident escalation and board-level visibility for higher-risk uses. The EU sustainability reporting framework is also evolving, following recent simplification reforms to the CSRD/ESRS framework, but the core expectation remains that material technology-related risks should be identified, managed and, where applicable, disclosed.

21. AI Governance and Compliance

21.1 AI Governance Frameworks and Implementation

Effective AI governance requires organisations to move beyond purely technical considerations and adopt a structured, risk-based approach that integrates legal, operational and ethical dimensions.

A starting point is a clear understanding of the specific use cases in which AI is deployed, typically supported by internal AI inventories and classification exercises that map systems according to their function and risk profile. This is operationalised through impact assessments, enabling organisations to anticipate issues relating to data protection, bias, transparency and system reliability at an early stage.

Compliance with applicable legal frameworks – most notably the AI Act and the General Data Protection Regulation – must be embedded into the design and life cycle of AI systems. This includes implementing appropriate governance structures (such as cross-functional oversight or risk committees), defining internal responsibilities and ensuring adequate documentation, monitoring and audit capabilities.

In Portugal, this approach is consistent with the National Artificial Intelligence Agenda, which emphasises responsible AI, risk assessment tools, AI literacy, regulatory sandboxes and the development of practical compliance guidance.

Organisations are also increasingly investing in AI literacy and internal capability-building, recognising that effective governance depends not only on formal controls but also on informed decision-making across business functions. Particular attention is required in the management of third-party AI systems, including due diligence, contractual safeguards and ongoing oversight of external providers.

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 Luke.Wilson@Chambers.com