Chambers
AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Artificial Intelligence 2024

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

Portugal: Law and Practice & Trends and Developments

Ana Rita Paínho and Ana Mira Cordeiro
Sérvulo & Associados

PORTUGAL

Law and Practice

Contributed by:
Ana Rita Paínho and Ana Mira Cordeiro
Sérvulo & Associados

Contents

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

2. Commercial Use of AI and Machine Learning 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.7
3.4 EU Law 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.8

4. Judicial Decisions p.8
4.1 Judicial Decisions p.8
4.2 Technology Definitions p.9

5. AI Regulatory Oversight p.9
5.1 Regulatory Agencies p.9
5.2 Technology Definitions p.9
5.3 Regulatory Objectives p.10
5.4 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.10

7. Government Use of AI 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 Emerging Issues in Generative AI p.12
8.2 IP and Generative AI p.13
8.3 Data Protection and Generative AI p.14

9. Legal Tech p.15
9.1 AI in the Legal Profession and Ethical Considerations p.15
10. Liability for AI p.15
10.1 Theories of Liability p.15
10.2 Regulatory p.16
11. Legal Issues With Predictive and Generative AI p.16
11.1 Algorithmic Bias p.16
11.2 Data Protection and Privacy p.17
11.3 Facial Recognition and Biometrics p.18
11.4 Automated Decision-Making p.18
11.5 Transparency p.19
11.6 Anti-competitive Conduct p.19
12. AI Procurement p.19
12.1 Procurement of AI Technology p.19
13. AI in Employment p.20
13.1 Hiring and Termination Practices p.20
13.2 Employee Evaluation and Monitoring p.20
14. AI in Industry Sectors p.21
14.1 Digital Platform Companies p.21
14.2 Financial Services p.21
14.3 Healthcare p.22
14.4 Autonomous Vehicles p.23
14.5 Manufacturing p.23
14.6 Professional Services p.23
15. Intellectual Property p.24
15.1 Applicability of Patent and Copyright Law p.24
15.2 Applicability of Trade Secrecy and Similar Protection p.24
15.3 AI-Generated Works of Art and Works of Authorship p.24
15.4 OpenAI p.25
16. Advising Corporate Boards of Directors p.25
16.1 Advising Directors p.25
17. AI Compliance p.26
17.1 AI Best Practice Compliance Strategies p.26

Sérvulo & Associados is a Portuguese full-service law firm with 20 years of existence, occupying a leading position in the Portuguese legal market. Widely recognised for the quality of its legal services in all relevant areas of law and strategic sectors, SÉRVULO has a highly competent multidisciplinary team of more than 100 lawyers, motivated by the purpose of transforming accumulated knowledge and experience in designing sound legal solutions in the benefit of its clients.

SERVULO'S TMT Team (with 8 members), led by Ana Rita Paínho, stands out in TMT. With practical and technical knowledge of the issues inherent to the technology industry, it provides legal and strategic advice on all relevant areas, including the software industry, e-commerce, the internet, and all matters related to new technologies, as well as regulatory issues in the telecommunications sector.

Authors

Ana Rita Paínho Head of the department, with more than 25 years of experience as a TMT specialist. Ana Rita assists on a broad spectrum of TMT matters, with particularly strong expertise in technology/IT (including IT contracts, software, internet and e-commerce), publicity and marketing and telecoms.

She acts for major names in the technology and telecommunications sectors and has considerable experience assisting international clients with local law issues. Ana Rita also handles TMT-related disputes.

Ana Mira Cordeiro Senior associate (top level), having over 24 years' experience in the fields of e-commerce and consumer protection, IP, TMTs, information society, software and Privacy and Personal Data Protection issues, and her activities have mainly focused on these fields. Apart from mainstream law firms and an in-house counsel to multinational companies and banks, Ana also worked with the national telecommunications regulator (ANACOM) for several years and, among other qualifications, has an LLM in International Trade and Business Law.

Sérvulo & Associados | Sociedade de Advogados, SP, RL

Rua Garrett
64 1200-204 Lisboa
Portugal

Tel: +351 21 093 30 00
Fax: +351 21 093 30 01/02
Email: geral@servulo.com
Web: www.servulo.com

Sérvulo & Associados | Sociedade de Advogados, SP, RL

1. General Legal Framework

1.1 General Legal Background

The recent enactment of the Artificial Intelligence Act ("AIA") by the European Parliament (approved March 2024, expected to enter into force by late April 2024) marked the first major comprehensive high-level legislative effort towards AI regulation, which is expected to deepen from 2025 onwards (companies have one year to adapt to AIA).

- *National background:* No specific national laws/guidelines have been enacted yet. As an EU Member, Portugal is subject to the immediate and direct application of European Regulations, the transposition of European Directives, and close regard for European Guidelines. As such, specific legislation (namely on privacy and data protection, IP, product safety, and consumer protection) was enacted with close proximity to European standards.

In addition to the direct applicability of the AIA, AI-based Systems must abide by:

- *Privacy and Data Protection Law:* AI (both generative and predictive) poses challenges due to potential user misuse, considering the nature of the learning models, the possibility of perverse inversion attacks, and data leakage. These issues can only be tackled with adequate regimes, strong data governance measures, and tailored (by design and default) privacy-enhancing solutions to ensure compliance with GDPR and EU guidelines.
- *IP Laws:* Generative AI holds major output on the legal issues raised; AIA focuses on the applicable standards for copyright protection due to the lack of a comprehensive range of legal solutions. This is particularly relevant to large language models ("LLMs") concerning the use of copyrighted text and materials in training datasets (in a knife-edge duelling with privacy and data protection, regarding web scraping as the basis of the machine learning model "ML"). Different interests of developers, content owners and users are poorly regulated in the face of the new means of *content creation, with various interpretations and potential legal gaps.*
- *Contract Law:* As the basis of most interactions, strong contracts provide legal clarity (on outputs, ownership of data, IP rights, and Data protection), which is particularly relevant in "grey", newly regulated areas/technologies, like broad-use AI Systems. For predictive AI, well-drafted T&Cs may dictate the terms for good practices on collecting, storing, and using data for ML, avoiding non-compliance repercussions.
- *Liability:* This is one of the major obstacles to the broad adoption of corporate AI. In the absence of specific national regulation, reference is made to two European-level projects:
  (a) amendments to the Product Liability Directive ("PLD"); and
  (b) AI Directive ("AILD"), both still under discussion. Challenges include defining the scope, assessing defectiveness and fault, and ensuring proper disclosure of evidence. Active disclosure of adverse effects by generative AI producers is advisable.
- *Labour:* AI is used to score employees when hiring but is not widely used for termination since individual grounds for termination must always be provided.

2. Commercial Use of AI and Machine Learning

2.1 Industry Use

Generative AI creates new data/content that resembles training data distribution, and its techniques are used to synthesise novel data samples. *Predictive AI* methods focus on making accurate predictions or decisions based on existing data/patterns.

Both systems can reproduce multiple realities due to several types of learning: supervised learning (where algorithms learn from labelled data to predict specific outcomes), unsupervised learning (by extracting meaningful patterns from unlabelled data), and reinforcement learning (optimising decision-making policies over time, often through trial and error).

AI's growing presence in day-to-day market solutions makes it hard to distinguish between key and general applications. A notable key application is management: almost all management tasks can be automated with valid input in predictive AI solutions, with faster and more efficient preventive response and reallocation of resources (scenarios from CRM to airport traffic management) and, in the case of generative AI, in automated customer messaging bots (in most advanced systems, bots can already include elements of generative and predictive AI).

Telecom companies are already implementing AI Systems by designing networks with predictive AI as a tool to improve operational efficiency by balancing the network's distribution and reducing operational costs.

2.2 Involvement of Governments in AI Innovation

National investment programs in AI innovation include:

- AI Portugal 2030 (INCoDe.2030): mobilisation of citizens and key stakeholders to develop a knowledge-intensive labour market, foster AI technology production and export, supported by research and innovation and ensure widespread availability of AI technologies to enhance efficiency, quality and fairness across all sectors, including SMEs, public services and education.
- Digital Innovation Hubs, Innovation Vouchers, Public sector AI projects and cooperative platforms.

There are no apparent differences between generative and predictive AI.

Although AI regulations differ globally due to cultural norms and legislative contexts, there is a progressive global involvement in AI innovation and the widespread adoption of national AI strategies. As of May 2023, governments reported over 930 policy initiatives across 71 jurisdictions in the OECD overview.

Several countries are forming multi-stakeholder groups of AI experts outside government to advise on current and future opportunities, risks, and challenges of AI use in the public sector, as well as AI observatories to oversee the implementation of AI strategies, indicating a trend that may expand, as other countries progress in their AI strategy implementation.

3. AI-Specific Legislation and Directives

3.1 General Approach to AI-Specific Legislation

AIA is the first and new EU AI-specific legislation to be implemented in the EU. It must be considered not only innovative but also groundbreaking. It was preceded by a complex process, starting with growing awareness of AI's transformative potential and societal implications.

The European Commission prioritised building a digital Europe, aiming to achieve digital transformation by 2030, focusing on digital skills, infrastructure, business transformation, and public services. Aligned with other high-level legal instruments (still to be fully enacted) as the Data Governance Act, Data Act, Digital Services Act, Digital Markets Act, complemented by NIS/NIS2 Directive and the Cyber Resilience Act, form a comprehensive legal structure aiming this purpose.

AIA focus primarily on:

- harmonised rules for placing on the market, putting into service and use of AI Systems;
- prohibitions of certain AI practices;
- specific requirements for high-risk AI Systems and obligations for operators of such systems;
- harmonised transparency rules for certain AI Systems;
- harmonised rules for the placing on the market of general-purpose AI models;
- rules on the market monitoring, market surveillance governance and enforcement; and
- measures to support innovation, focusing on SMEs and start-ups [AIA, Article 1(2)].

In view of national interests outlined in the AI Portugal 2030 strategy, Portugal may enact further solutions to oversee high-risk AI applications, potentially fostering a more favourable environment for certain types of AI development.

While predictive AI, which relies on algorithms to forecast future outcomes based on historical data, could face heightened government scrutiny, generative AI - capable of producing new content like images or text - might experience fewer restrictions unless deployed in high-risk scenarios.

3.2 Jurisdictional Law

Portugal has not yet enacted AI-specific legislation. Once enacted, the AIA will directly apply in Portugal (see above).

Given Portugal's past experience, framing legislation will align with EU trends. Portuguese legislators usually have strong concerns regarding privacy and personal data (sensitive data: health data and biometrics), and in the context of labour relationships, which may result in stricter obligations or security measures, further conditioning criteria, and surveillance of AI Systems used in these fields.

3.3 Jurisdictional Directives

Portugal's most active authorities in the AI field (CNPD – the Data Protection NRA), ANACOM – the Telecom NRA and the National Artificial Intelligence Strategy) have not yet issued guidelines or recommendations in AI.

Under the EU Digital Action Plan, the strategy promoted by INCoDe.2030 defined various objectives up to 2030. However, these do not include guidelines on the regulation or use of AI Systems, rather focusing on programmes encouraging digitalisation of companies and innovation in the sector.

3.4 EU Law

3.4.1 Jurisdictional Commonalities

Being a Regulation, when enacted AIA will be immediately enforceable in all member states; thus significant deviations will not be possible. Still, EU Regulations typically require additional implementation measures to ensure full compatibility within the national legal framework.

EU Directives require a binding and enforceable transposition process through acts of the national parliament or government, incorporating provisions into the Portuguese legal system. Additionally, national authorities are responsible for monitoring compliance with EU regulations and ensuring their enforcement at the domestic level in coordination with EU institutions and guidelines.

Portugal has not yet enacted AI-specific legislation, but it usually does not deviate from overall EU guidelines and commonly assumes strict positions in these matters.

3.4.2 Jurisdictional Conflicts

Portugal has not yet enacted AI-specific legislation or guidelines; hence, there are no immediate inconsistencies or contradictions with current EU legislation and underlining principles, and this is not expected to occur.

3.5 US State Law

Only applicable in the US.

3.6 Data, Information or Content Laws

Portugal still needs to enact AI-specific legislation and guidelines; full enactment of the AIA is expected. Once this occurs, national framing legislation will be revised to accommodate and align with EU regulations.

Local public bodies have not yet issued additional recommendations or directives in this regard, including non-binding.

3.7 Proposed AI-Specific Legislation and Regulations

The most relevant pending AI-specific legislation is the AIA on the EU level. A national internal implementation shall follow EU guidelines, adapting the national legal framework accordingly.

AIA could significantly impact predictive AI. If, based on a case-by-case analysis, these systems are deemed high-risk, they could be subject to stricter government oversight by national NRAs, potentially slowing down their development and deployment. Generative AI may be less impacted and escape stricter regulatory requirements unless used in high-risk applications, but it will still be affected by Data Protection and IP regulations.

Potential impacts will depend on the interpretations of AIA and if (and how) Portugal chooses to complement/execute it.

4. Judicial Decisions

4.1 Judicial Decisions

Portuguese courts have not yet dealt with AI-related matters. National courts are expected to align with the jurisprudential trends of other EU jurisdictions.

Despite an apparent increase in the number of cases brought before international courts addressing AI Systems, case law on the subject is still very recent (notably (i) UK: Thaler v. Comptroller-General of Patents, Designs and Trademarks (December 2023); and (ii) US: several federal class action lawsuits filed against prominent generative AI developers, such as OpenAI and Google).

Existing cases tend to focus on privacy and copyright infringement issues, focusing on generative AI developers. The key issue is whether the collection and use of publicly available data, possibly subject to copyright protection, for training AI models constitutes infringement.

Courts have been reluctant to impose liability on AI developers, demanding more specific, factual, and technical details. However, the legal landscape of generative AI is still evolving, and the coming months will be pivotal in shaping the future direction of AI litigation.

As generative AI continues to develop and become widely used, companies adopting it should ensure that they understand the risks associated with data collection and usage and take proactive measures to mitigate potential legal risks.

4.2 Technology Definitions

Portuguese courts have not yet dealt with AI matters. One key point from the high-level analysis of foreign decisions is the courts' approach to generative or predictive AI, specifically regarding IP.

A relevant issue shall be the interpretation of the "AI System" concept in the AIA (Article 3(1)) in relation to the content generated and the level of autonomy.

5. AI Regulatory Oversight

5.1 Regulatory Agencies

Regulatory authorities have not yet been appointed.

The NRA for Communications (ANACOM) is expected to act as market surveillance authority. It is possible that competencies regarding high-risk AI Systems may be shared (or derogated) to the NRA competent in Personal Data (CNPD) (see the AIA, Article 63(3) Annex II).

5.2 Technology Definitions

Portuguese legal system (including NRAs) still needs to define AI.

The AIA defines *"AI system"* as *"a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"* (Article 3 (1) AIA).

This broad definition encompasses both generative and predictive AI. With the upcoming enactment of the AIA, this definition shall prevail in EU jurisdictions.

Different definitions (namely from the Organization for Economic Cooperation and Development – OECD, with a more functional approach), if contrasting, may lead to inconsistency in AI regulation and enforcement, creating uncertainty in international trade by raising issues for businesses operating in multiple countries: namely, a company using predictive AI may be subjected to different regulatory scrutiny and obligations in different jurisdictions, being crucial for businesses to understand and adapt around these specificities.

5.3 Regulatory Objectives

No regulatory agency has yet been appointed to assume competence regarding AI market surveillance. Nevertheless, the currently existing NRAs are expected to continue to exercise their powers under their competencies if AI impacts them:

- CNPD – personal data and GDPR enforcement;
- ANACOM – telecommunications and e-commerce;
- Competition Authority (AdC) – impact on market competition; and
- Consumer Protection Agencies – consumer rights protection.

5.4 Enforcement Actions

No enforcement actions are known to date for AI.

Certain aspects of AIA are infringements that are administrative offences punishable with fines. The severity, duration, and consequences of the infringement, as well as the size of the provider, are determined on a case-by-case basis.

Namely, fines (Article 71 and 72 AIA):

- non-compliance with prohibited AI practices: up to EUR35 million or 7% of total worldwide annual turnover for the preceding financial year if the offender is an undertaking;
- non-compliance by an AI System with provisions related to operators or notified bodies: up to EUR15 million or 3% of its total worldwide annual turnover for the preceding financial year if the offender is an undertaking;
- supply of incorrect, incomplete, or misleading information to notified bodies or national competent authorities in reply to a request up to EUR7.5 million or up to 1% of its total worldwide annual turnover for the preceding financial year if the offender is an undertaking;
- for providers of general-purpose AI models: up to EUR15 million or not exceeding 3% of their total worldwide turnover in the preceding financial year.

6. Standard-Setting Bodies

6.1 National Standard-Setting Bodies

Portugal does not yet have government standard-setting bodies regarding AI.

Portugal recently underwent elections with a governmental change. The political programmes of the various parties provided insight into their national-level priorities, and overall, there seems to be no specific plan in place for the governance, ethics, and strategic development of AI, aside from transposing the upcoming European legislation and the previous national AI strategy.

Few concrete mechanisms are outlined to implement ethical, impartial, and secure AI Systems in alignment with emerging European regulations, and tangible guidance on AI governance or initiatives to monitor its social impact is still lacking. Future implementation of the AIA is paramount.

6.2 International Standard-Setting Bodies

Portugal has not enacted guidelines on AI, but implementation of the AIA is expected.

AIA will be directly applicable, and Portugal is usually well aligned with EU directives and guidelines, as issued by EU's standard-setting bodies, namely:

- *"Ethical Guidelines and the Assessment List for Trustworthy AI"* by an independent expert group set up by the European Commission;
- European Parliament resolution of 16 February 2017 on possible developments and adjustments to the current institutional framework of the EU;
- European Parliament resolution of 20 October 2020, with recommendations to the Commission on a civil liability regime for artificial intelligence.

Some other jurisdictions have chosen a sectorial approach, focusing on non-binding principles or sandboxes (namely the US and the UK), which are not expected to have an overall determining impact soon in the Portuguese or EU jurisdictions.

Other international standards may be of relevance (namely (i) the International Organization for Standardization published ISO/IEC 42001:2023, providing guidelines for implementing AI management systems (AIMS), aiming to increase the level of AI compliance; and (ii) the Bletchley Declaration – AI Safety Summit, a collaborative effort, signed by 28 countries, underscoring international cooperation's importance in unlocking AI's potential benefits while ensuring safety), but these shall serve as framing guidelines only.

Companies doing business in Portugal should embrace present and future guidelines issued by European-level bodies, considering the potential impact of enforcement actions by local NRAs.

7. Government Use of AI

7.1 Government Use of AI

Portugal enacted the Strategy for the Digital Transformation of Public Administration 21-26, proposing exploiting the potential of the enormous volume of data to which Public Administration ("PA") has access to provide better public services, manage and make decisions, and increase transparency.

Various public service portals, such as ePortugal, already use AI tools, such as the Sigma chatbot, which helps citizens find the information they need on the portal. The "Virtual Assistant," with recourse to Azure OpenAI Service, was presented in May 2023 as an AI tool for the public sector. It supports citizens' digital interaction with public services, taking advantage of voice and natural language processing.

However, there are huge challenges to the development and use of AI in the PA, particularly in terms of competencies, responsibility, ethics and participation, perception and acceptance by society.

PA is also subject to GDPR, thus limiting the use of facial recognition and biometrics. The main exceptions concern processing personal data to prevent threats to internal and external security, maintain the unity and integrity of the democratic rule of law, and safeguard the independence and national interests — which is regulated by other complementary legislation without specific mention of AI.

7.2 Judicial Decisions

There are no national decisions nor currently pending cases in Portuguese courts regarding the use of AI Systems by the public administration.

7.3 National Security

AIA does not apply to AI Systems for exclusive military, defence or national security purposes.

Article 4(2) TEU and the specificities of Union defence policy justify the exclusion of AI systems from military and defence activities. Public international law is a more appropriate legal framework for regulating AI Systems in these activities, including the use of lethal force.

The National Republican Guard ("GNR") already uses AI applied to geographic information systems, specifically terrain risk models, to analyse the risk of criminal phenomena, enabling better decision-making and proactive balancing of the institution's resources to combat them.

From the publicly available information, it is also possible to conclude that the Ministry of Defence and the Portuguese Armed Forces are involved in projects that include Artificial Intelligence. However, more detailed information is not available.

8. Generative AI

8.1 Emerging Issues in Generative AI

Generative AI introduces several ethical dilemmas, namely related to misinformation, privacy breaches, IP infringement, bias and discrimination. The potential for creating false content ("fake news"), leveraging personal data without consent, perpetuating biases and discrimination and infringing on intellectual property rights/copyright reinforces the importance of ethics guidelines for a trustworthy AI, supported by an underlying strong regulatory framework.

Addressing technical issues such as bias mitigation, transparency, and accountability in AI Systems requires robust mechanisms for auditing, evaluating, and enhancing model performance. Transparency regarding data sources, training methods and tailored parameters is essential for building trust and accountability. The principles already set forth by the AIA are strong guidelines towards this objective.

Protecting IP rights under AI and its assets, including models and training data used, input and output, depends, in addition to a strong and updated legal framework, on implementing strong and clear IP protection strategies by all interested parties, such as copyright registration and robust licensing agreements with tailor-made contractual provisions. The future T&Cs set by AI tool providers will play a significant role in determining the extent of IP rights and potential infringements.

High-level risks:

- Concept of "intellectual creation" applied to AI: current difficulty of establishing a clear form of protection for outputs produced by/through *'artificial agents or robots';*
- The possibility that, during training, AI Systems with recourse to web scrapping or another form of massive data collection include wordings or any other materials protected by copyright;
- Prompts used to guide the AI's operations and output generated by the AI: providers claim rights over the output generated by their AI, potentially restricting users' rights to the AI's output.

As for Data protection concerns, GDPR establishes several principles aiming to protect data subjects, including requirements of lawfulness, fairness, purpose limitation and transparency in personal data processing, along with several rights granted to data subjects, such as the rights to rectification, deletion and data portability, all also applicable to AI. Data protection rules are deemed to impact the use of AI technologies, and once these principles can be challenging to reconcile with generative AI Systems' broad and extensive data requirements, they also require transparency of AI Systems.

Adhering to purpose limitation and data minimisation principles is essential for mitigating privacy risks associated with generative AI and ensuring compliance with GDPR.

8.2 IP and Generative AI

In addition to AIA provisions, IP rights on the software and source code of AI Systems are protected under the existing national and European frameworks.

EU Directive 2009/24/EC was transposed in Portugal through Decree-Law 252/94 in connection with the applicable provisions of the Code of Copyright and Related Rights ("CDADC"). Although none of these laws contain provisions on IA Systems, their application has no immediate legal deterrents.

International standards, namely the Berne Convention and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), establishing minimum standards for copyright protection, must also be considered.

Training data: Directive 2019/790/EU ("DSM") may be applicable to Large Language Models ("LLMs") as a potential regulatory solution for training datasets in the context of text and data mining ("TDM"). However, this solution may be difficult to consider once:

- TMD is not carried out by research organisations but by companies with commercial purposes;
- the conditionthat their right holders have not expressly reserved the use of works (and other subject matter) in an appropriate manner, such as machine-readable means in the case of content made publicly available online; and/or
- a strict approach of Article 4(1) of the DSM would result that all data collected during the training phase were deleted and not used for the validation and testing phase (this being the most debatable since it is possible to argue a broad definition of TMD, which encompass the validation and testing phases).

In an LLM scenario, outputs can result in 3 characterisations: (i) infringement of IP rights due to the pre-existing materials (as above), (ii) qualification as derivate creations, and (iii) autonomous creations. This cannot be assessed in general terms; it can only be assessed on a case-by-case basis.

Robust and tailored T&Cs are paramount to protecting input and output generated by AI Systems.

Even in cases where the entire training process used lawful data under the GDPR and DSA, assuming that the training materials would not be expressive enough to be considered the basis of the outputs, the system's T&Cs may still be an impediment if they provide for some form of copyright on the final outputs.

LLMs in a training phase should only access information to which explicit consent has been provided or have a legal safeguard for its use. This is nearly impossible when assessing training through *web scraping* techniques due to the extensive number of users/copyright information. The following should be considered:

- the terms of web scrapping should be safeguarded with privacy by design and default mechanisms; and
- training data should be used in a controlled environment in accordance with the GDPR and other applicable legislation.

To this date, one of the key features is configuring AI Systems to analyse T&Cs to detect, prior to gathering information, if the specific T&Cs have clauses that prohibit web scrapping. Open AI established a technical tool that enables website owners to opt out of content access for web scrapping. This is an example of how IP potential infringements can be prevented or partly mitigated.

8.3 Data Protection and Generative AI

The current legal framework for personal data protection (GDPR, national implementation laws, and DSA) also applies to AI systems environments.

GDPR-compliant generative AI Systems are one of the major roadblocks. This is particularly challenging regarding information duties and the exercise of rights by data subjects.

GDPR allows data subjects to request the deletion of their data. As for generative AI (LLMs) this may require the deletion of the entire AI model if it's impossible to remove individual data points. However, the practical implementation of this right by AI models, which learn from the data but do not necessarily store it, is a complex issue that is still under heavy debate.

The AI System operator must implement mechanisms to correct inaccurate data. However, the technical implications of assuring, with a high level of confidence, the ability to erase and/or rectify specific data as granted by the GDPR from an AI model without deleting the entire learning set are considerable and still dubious. Challenges for data limitation and minimisation are no less once consent can serve as legal ground for processing data input by the user; the same does not apply when the user inputs personal data from a third party.

Compliance with all relevant GDPR principles presents significant challenges, as AI Systems require large amounts of data and may produce outputs that go beyond the original purpose of data collection. Companies must implement strict data governance and management practices, including transparent data collection, use and storage policies and robust mechanisms for obtaining and managing consent.

Article 10 of AIA requires specific mapping regarding data governance:

- good design phase (assessment of quantity, suitability, contextual behaviour, including a preliminary analysis of possible biases);
- development phase with due consideration of the GDPR regarding data collection, validation step (relevancy, correctness of information) and specific development with adequate data preparation and precise measures to mitigate possible biases;
- testing (auditing compliance gaps and mitigation measures);
- deployment, ensuring data maintenance, relevancy, representativeness and validation.

9. Legal Tech

9.1 AI in the Legal Profession and Ethical Considerations

The Portuguese Bar Association addressed AI at its last congress (July 2023) but did not release any guidelines.

AI Systems in legal practice are gaining ground, being used to review contracts, document analysis in DDs and help manage client billing time. Most top-tier law firms in Portugal are investing in internal AI Systems, comprising (i) legal document analysis, (ii) internal LLMs for general and client-specific purposes, and (iii) legal research.

By aligning ethical standards laid down both at the national level and in the Code of Ethics for European Lawyers, the essential keynote is that the use of AI Systems should always be made from a complementary point of view. Whether in a scenario of predictive AI (for predicting legal outcomes) or generative AI (drafting or document analysis), the discussion amounts to correctly applying compliance systems in terms of personal data, preventing situations of breach of confidentiality or other forms of violation of professional duties.

Compliance with GDPR, consumer protection, and the AIA is crucial for safeguarding user rights, ensuring transparency and addressing potential IP infringements.

This special focus is due to the ethical use of AI in protecting fundamental rights, democracy, and the rule of law, as well as high-risk AI Systems, which could include specific applications of Generative AI. Key provisions include transparency (Articles 13, 52), user information (Article 53), and robustness and accuracy requirements (Articles 15, 13, 16). The AIA also emphasises human oversight (Article 14) and accountability (Article 17).

10. Liability for AI

10.1 Theories of Liability

Most EU-based legal systems rely on the premise that liability falls upon the direct infringer/causer of the damage. The general rules on subjective liability typically require proof of an action or omission, whether negligent or wilful (breach of contract or “wrongful act”), attributable to the person (natural or legal) who caused the damage, along with the corresponding causal link.

Considering the current legal framework, insofar as a direct causal link may be established between a “responsible” for the act causing the damage – either responsibility for programming, development, establishing patterns and guidelines for inputs and outputs, distribution, placing into the market, etc – the frame of the same principles for AI Systems.

When applied to AI Systems, these well-established rules may be difficult to uphold once when AI comes between a person’s action/omission and the damage, the specific characteristics of certain AI Systems, such as opacity (black box effect), autonomous behaviour and unpredictability, can make it excessively difficult or even impossible to determine immediate authorship of the infringing conduct, and for the injured party to fulfil its burden of proof.

Current rules on producer and supply chain liability are based on the principle that the producer (broadly defined along the distribution chain) is liable for damages caused to the final user/consumer by the defect of a product that it has put into circulation.

Although it may be difficult to classify IA Systems as a "product" under the existing principles on liability for defective products (Directive 85/374/EEC), still a similar solution may be envisaged, sustained by more recent principles on consumer protection and liability within the supply chain (Directive 2011/83/CE).

AI Systems are not — and may not — be considered legal persons who do not have autonomous legal personalities, namely for liability purposes. But despite the particularities of AI Systems, considering the current principles, a solution where the ultimate responsibility for actions resulting from AI Systems is committed to the business selling or providing AI products or services will be the most reasonable when the protection of users/consumers is at stake.

Considering the risks associated with autonomous actions, the implementation of compulsory insurance obligations to AI Systems providers is a relevant solution to consider.

10.2 Regulatory

There are currently no legislative initiatives envisaged in Portugal regarding specific liability for AI. As a member of the EU, liability for AI will involve the transposition of future European directives, namely:

- AIA complementary laws;
- Proposal amendments to Product Liability Directive ("PLD II");
- Proposal for Artificial Intelligence Liability Directive ("AILD").

The key points intended in the new European Framework aim to (i) facilitate legal proceedings and enhance safeguards for individuals affected by AI Systems by reducing the evidentiary requirements for victims and aiding them in accessing evidence (reverse the "black box" effect) and (ii) promote growth in the AI market by bolstering consumer confidence, ensuring greater assurances and offering more explicit legal guidelines for businesses.

Matters relating to defectiveness, fault assessment, and evidence disclosure persist. Technical work, in addition to legislative work, needs to be done to ensure that these regulations are effective in responding to the nuances of generative and predictive AI.

11. Legal Issues With Predictive and Generative AI

11.1 Algorithmic Bias

While various regulatory bodies worldwide have acknowledged the importance of collectively addressing algorithmic bias, there is a notable absence of specific legislation or regulations dedicated to this issue. Bias in this context refers to situations where AI Systems' outcomes disproportionately favor or discriminate against specific ideas, groups or individuals, potentially leading to unlawful discrimination. This may seriously affect certain categories of individuals, more fragile or susceptible to discrimination (regarding sex, sexual orientations, race, religion, political stands, minors, etc).

Within the EU context, AIA primarily addresses mitigating risks associated with discrimination linked with biased algorithms, even though it does not explicitly mention bias prevention. AIA includes mandatory requirements for high-risk AI Systems concerning risk management, data governance, technical documentation, oversight, conformity assessment and accuracy, all of which play a crucial role in safeguarding against bias and discrimination.

AIA also emphasises the need for explainability in AI Systems, requiring organisations to clarify how data, models or algorithms were used to reach specific outcomes and justify their methods.

For companies using AI Systems, emphasis on explainability and transparency is crucial, particularly in cases where AI decisions face scrutiny for potential discrimination. Thorough record-keeping in the AI System's lifecycle can serve as evidence of nondiscriminatory decision-making.

Although European regulations such as the European Convention on Human Rights (ECHR) and the GDPR may offer frameworks for addressing discrimination, it remains uncertain whether these laws are sufficiently broad to effectively tackle the challenges posed by algorithmic bias and discrimination in the future. Since there is still no legislation or proposals for specific legislation, the solution will always be to combine the principles set out by AIA with existing EU legislation.

11.2 Data Protection and Privacy

Protection of personal data on AI technology has the following.

Benefits

Key benefits stemming from it are (i) ability to provide personalised services and experiences; (ii) increase efficiency and reduce costs.

AI Systems can analyse users' behaviour, preferences, and past interactions to provide relevant content and recommendations, improving user satisfaction and engagement and leading to better business outcomes.

Risks

Enlisting AI's help in processing large amounts of personal data does not come without its caveats. If not properly designed and managed, such data processing could be deemed illicitly accessed or misused, leading to security breaches. Moreover, using AI for automated decision-making can lead to biased or unfair decisions.

As a rule, fully automated individual decision-making, including profiling that has a legal or similarly significant effect, is forbidden [Article 29 Data Protection Working Party; Guidelines on Automated Individual Decision-making and Profiling for the purposes of Regulation 2016/679].

The same principles are applicable to processing machine-generated data without direct human oversight (Article 14 (2) AIA), which can lead to similar risks.

Human involvement cannot be bypassed by controllers. While automated processing can increase efficiency and reduce costs, it can also lead to errors, discrimination or biases if the AI System is incorrectly designed or monitored. These risks can be mitigated through proper data governance, including transparency and regular performance audit.

Data security

Safekeeping of the processed information is another critical aspect of AI Systems. Given the often sensitive nature of the data handled, implementing robust security measures to prevent unauthorised access and data breaches is paramount. This includes practices such as encryption, access controls, and regular security testing.

While AI technology has the potential to provide significant benefits, it is essential to carefully manage the associated risks, especially when it comes to personal data. This requires a comprehensive approach prior to implementation, envisioning specific objectives, robust data governance, transparency, IP protection and strong data security measures.

11.3 Facial Recognition and Biometrics

Under GDPR (Article 9), facial recognition and biometrics are deemed sensitive data; thus, general processing is forbidden and only possible in specific and justifiable circumstances. In Portugal, Law 58/2019 (complementing GDPR) provides stricter guidelines, determining that biometrics in the labour context (fingerprints, facial recognition) can only be used for purposes of attendance and access control to the employer's premises.

CNPD has adopted a conservative approach and maintains a very stringent viewpoint, issuing an opinion (Opinion 2021/143) expressing very restrictive views on the use of video surveillance images and personal data resulting thereto (even within the scope of public safety and crime prevention), also expressing concerns about potential future uses, such as the use of drones, AI, the capture of biometric data and the overall use of cameras in public and the use of images, all within the context of privacy protection and restricted use of personal data.

There are exceptions for criminal investigation (fingerprints), but no advanced facial recognition programs for live video surveillance are available.

Non-compliance with the applicable rules consists of administrative offences punishable with fines under GDPR.

11.4 Automated Decision-Making

Technology within Automated Decision-Making ("ADM") in AI Systems involves the use of ML algorithms and other models to make decisions without human intervention (credit scoring, disease diagnosis, personalised advertising). These systems can recur to neural networks, decision trees or natural language.

There are several enacted regulations, in particular:

- GDPR:
  (a) Controller must provide the data subject with additional information to ensure fair and transparent processing:
    (i) the existence of automated decisions, including profiling [Article 22(1) and (4)]; and
    (ii) useful information concerning the underlying logic as well as the significance and envisaged consequences of such processing for the data subject [Article 13(2)(f), 14(2)(g) and15 (1)(h)].
  (b) Right not to be subject to any decision solely based on automated processing, including profiling, which produces effects in the legal sphere (or in similar ways), without prejudice of the exceptions foreseen.
- AIA:
  (a) High-risk AI Systems used for ADM must meet specific requirements, including transparency (Article 13 AIA), human oversight (Article 14 (4) (b) AIA), and robustness (Article 15 AIA). They will also be subject to third-party conformity assessments (Article 6 (b) AIA) for medium-risk and high-risk products.

Non-compliance with the above obligations could result in administrative offences, both under GDPR and AIA (Article 83 and Articles 71 and 72, respectively).

11.5 Transparency

AIA aims to strengthen the effectiveness of existing rights and remedies by establishing specific requirements and obligations, including transparency (full disclosure towards users of AI Systems and its particularities), technical documentation to be made available and disclosed and record-keeping of AI Systems [Recital (5a) AIA].

Transparency means that AI Systems must be developed and used in a way that allows appropriate traceability and explainability while making humans aware that they communicate or interact with an AI System. Deployers must also be duly informed of the capabilities and limitations of that AI System and affected persons about their rights [Recital (14a) AIA].

All AI Systems that are considered high-risk must comply with the provisions of the AIA, namely, Article 13 and Title IV, for AI Systems intended to interact with natural persons directly.

Failure to comply with transparency obligations is subject to administrative offences, punishable with fines (see **5.4 Enforcement Actions**).

11.6 Anti-competitive Conduct

Key issues for competition and antitrust law concerning price-setting using AI technology:

- Discriminatory conduct: companies with generative AI may discriminate against competitors by limiting access to data or cloud computing services. Established companies may also use their dominant position to disadvantage competitors by providing unfavourable API access to protect their market standing.
- Price collusion through price monitoring and matching algorithmic software: companies using price matching and monitoring algorithmic face obstacles due to prohibitions on sharing information with competitors.
- Algorithmic collusion: several algorithmic theories of harm have been identified, encompassing algorithmic collusion, algorithmic unilateral conduct and algorithmic exploitative conduct (including unfair trading practices, price discrimination, and excessive pricing).

EU Competition Law prohibits explicit and tacit collusion and abusive behaviour by companies holding a dominant position in any given market under Articles 101 and 102 of the TFUE. In addition, National competition authorities can request information from companies in cases of suspected breach of competition regulations. DMA empowers the Commission to monitor specific obligations and measures outlined [Article 26(1)].

12. AI Procurement

12.1 Procurement of AI Technology

Although AI will change some paradigms, most will not be a revolution but an adaptation of the already existing practices, namely as resulting from online business; the same applies to procurement.

The main existing concerns about procurement of other services/products should simply be reinforced. More specifically:

- delimitation of the system’s learning and content sharing model;
- level of compliance with European standards;

- respect and enforcement of data protection guidelines and IP rights;
- warranty and general security assurances; and
- strengthen of security measures on identification and verification of binding powers.

Companies should take particular care with the contracts concluded, avoiding generic user licences or simple adhesion contracts.

13. AI in Employment

13.1 Hiring and Termination Practices

There are no tools that are forbidden regarding the hiring and termination of employees. To lower the risks of discriminatory decisions, the Portuguese Labour Code (PLC) imposes obligations on Employers:

To keep a register of recruitment procedures including the following information, broken down by gender:

- a) Invitations to fill posts;
- b) Job vacancy adverts;
- c) Number of applications for curricular assessment;
- d) Number of candidates present at pre-selection interviews;
- e) Number of candidates awaiting admission;
- f) Results of admission or selection tests;
- g) Social balance sheets with data that enables the analysis of possible discrimination against people of one gender in access to employment.

Termination without cause (either subjective or objective) is forbidden, and the written grounds for termination must be provided.

The employer is required to notify the Commission for Gender Equality when opposing the renewal of a term contract if the employee is pregnant, enjoying parental rights, or an informal carer.

13.2 Employee Evaluation and Monitoring

PLC forbids the use of remote surveillance tools to monitor employee performance. Use of electronic surveillance is allowed only where required to/by:

- protection and safety of people and property; and
- the specific requirements for the activity pursued.

CNPD issued guidelines that prohibit the systematic tracking of the employee's activity, including the use of software that registers the web pages visited, real-time terminal location, use of peripheral devices (mice and keyboards), capturing desktop images, observing and recording when access to an application starts, controlling the document the employee is working on, and recording the time spent on each task.

Law 58/2019 of 8 August 2019 provides that data collected through remote surveillance can only be used in disciplinary action to the extent that the employee engaged in criminal conduct. Biometric data may only be used to access the company's premises and control attendance.

Electronic Monitoring is subject to prior Works Council (WC) advice.

14. AI in Industry Sectors

14.1 Digital Platform Companies

AI is already being used on multiple business, especially those addressed to provision of consumer services in a relevant scale, namely by platform companies providing car travel and food delivery services.

The use of AI Systems in these business models clearly improves customer experience, with tailored options (personalised menu recommendations and destination locations, for instance), based on the analysis of customer's preference, order history and past behaviour.

The use of these tools, although widely spread and admitted, must always comply with GDPR, general consumer protection, cybersecurity and privacy rules, as well as with AIA.

As for employment regulations, AI Systems under the scope of an ADM system will not be acceptable for now under GDPR and the Portuguese Employment Code.

On the replacement of human jobs with AI tools, the national strategy for empowering employers issued programmatic provisions on complementary training to enable replaced workers to find new activities.

14.2 Financial Services

The Portuguese financial services sector is undergoing transformations driven by AI Systems, largely empowered by the use of Big Data, ML and LLMs, being the epicentre of several modifications in firm-client relations. Main use relates to risk management models, namely in AML/CFT and fraud detection, payments monitorisation, credit risk management (client scoring and anticipation of events of default by using Internal Ratings-Based models), robo-advisors and algorithmic trading.

The use of AI Systems substantially improves clients' and investors' services by more efficiently offering financial products and services, but it also poses risks connected with cybersecurity, data vulnerability, explainability, and the influence of behavioural biases.

Portuguese legal system does not yet include specific regulation designed to address the usage of AI in financial services; thus consisting of the adaptation of pre-existing rules in national and European financial services and banking legislation (ie, Portuguese Securities Code, Legal Framework of Credit Institutions and Financial Companies, Law 83/2017 on AML/CFT prevention measures, MiFID II, Market Abuse Regulation and GDPR).

In the absence of a comprehensive regulatory framework, supervisory authorities (Portuguese and European) and relevant stakeholders are starting to develop AI-specific governance principles and guidance for financial firms. In 2023, the Portuguese Institute of Corporate Governance (IPCG) revised the IPCG Code, introducing a new recommendation addressing the use of AI mechanisms.

With AIA, the legal vacuum is expected to change rapidly since it specifically addresses the financial sector; namely, evaluating a natural person's creditworthiness (CWA) and credit scoring activities are included in the list of high-risk use cases, subject to stricter rules.

Directive (EU) 2023/2225 on Consumer Credit (pending transposition in Portugal) addresses the interaction of CWA activities with the GDPR, prohibiting the use of certain personal data for creditworthiness assessment.

DORA (applicable to all EU Member States from 17 January 2025) shall ensure that the financial entities are able to resist, respond to and recover from disruptions and threats related to information and communication technology.

14.3 Healthcare

Specific AI Systems in this regard are but a few. However, AI is already revolutionising healthcare by aiding in patient treatment, monitoring health data on a large scale, and aiding in drug discovery. Its ability to systemise data and improve disease diagnosis early is increasingly recognised by the scientific and clinical communities.

In Portugal, a digital symptom evaluator accessible through the CUF mobile app enables patients to respond to a series of questions to receive potential diagnoses for referral, serving as an initial assessment. In early 2024, the National Health Service (NHS) introduced a funding initiative for the integration of AI tools in dermatological diagnoses: through an app, individuals take a picture of their skin condition and forward it to a dermatologist for review, reducing in-person consultations. Also, the National Strategy for the Health Information Ecosystem (ENESIS 2022) aims to propel the digital transformation of Portugal's healthcare sector and develop Health Information Ecosystem (eSIS) through the activity plans of the SPMS and other entities.

These applications may involve software as a medical device ("SaMD") and related technologies like ML algorithms, whose data use and sharing is now subject to regulation under AIA. ML is pivotal in digital healthcare, offering the ability to learn from data and enhance performance over time. Nonetheless, it entails risks of:

- Bias: if the training data is biased or not adequately representative, the AI System may generate biased or erroneous outcomes (AIA provisions on bias detection, Article 10(5) and human oversight, Article 14 AIA).
- Transparency: training, validation and testing datasets must be relevant, sufficiently representative and to the best extent possible, free of errors and complete in view of the intended purpose (AIA Article 10(3)).
- High-risk AI Systems must be designed and developed to ensure that their operation is sufficiently transparent to enable deployers to interpret the system's output and use it appropriately (AIA Article 13 (1)).

Robotic surgery comes with associated risks that can be divided into those directly linked to the use of the robotic system and the general risks inherent in the surgical procedure itself. The precision of robotic control relies on the reliability of the data connection between the surgery, and like all mechanical and electronic devices, surgical robots are susceptible to malfunctions.

Centralised Electronic Health Record ("HER") systems offer the potential to streamline data sharing for ML purposes, which can be seen as beneficial. However, it also raises important concerns regarding data privacy and cybersecurity. Without adequate protection, these systems are vulnerable to cyber-attacks, endangering patient privacy and the integrity of patient's personal data.

All AI developments in healthcare comes with risks, specifically concerning patient safety, data privacy and protection of patient's personal data, since AI Systems often rely on large datasets encompassing personal health information, potentially introducing concealed biases.

EU companies developing software/medical devices powered by AI that process the personal data of patients must abide by GDPR and, in the future, by AIA, taking into special consideration that health-related data is sensitive data, subject to stricter restraints.

14.4 Autonomous Vehicles

Autonomous vehicles powered by AI are subject to various regulations and standards that govern their operation, safety and data collection; often intersecting transport and technology law and vary by jurisdiction. Data privacy, security and liability are significant concerns.

Autonomous vehicles collect vast amounts of data, some of which can be personal or sensitive. Protecting this data is crucial to comply with privacy laws like under GDPR and to maintain user trust.

Portugal has yet to enact specific liability dispositions applicable to autonomous vehicles. However, under general principles, only a fully autonomous vehicle (ie, without an "on/off button") would create a really new legal problem, which, according to publicly available data, will not happen soon.

If human command is possible, the provision contained in Article 503(1) of the Civil Code continues to provide framing of liability for damage caused by land vehicles: if the user of any type of such vehicle has a choice between operating it manually or using the autopilot, the domain of use remains.

Future transposition of the European Directives on liability in AI Systems will ease the proof requirements in such cases. Now, given the legislation in force and the state of development of autonomous vehicles, verification will always be on a case-by-case basis, checking the degree of autonomy of the vehicle and the specific circumstances of the events that caused the damage.

14.5 Manufacturing

AI, in both neutral deep learning networks and ML solutions, is gaining prominence, allowing for a higher level of production automation. Even in cases where AI Systems are not specifically applied to automation (replacing workers), they are already being used as resource management solutions, making it possible to manage waste, logistics, costs, etc.

One of the most important major changes in "Industry 4.0" is the so-called collaborative robots, trained with spatial notions and without programming limitations on repeating the same function. These robots allow humans and robots to coexist in the factory. The AIA [Recital (28)] already mentions that this type of machine *"should be able to operate and perform their functions in complex environments safely."*

It should be noted that the AIA does not exclude European product safety and data privacy regulations [Articles 5a and 5b].

14.6 Professional Services

In Portugal, there are still no regulations governing the use of AI in professional services.

The introduction of AI in the workflows comes with an aggravated duty of responsibility to ensure that confidentiality duties and professional obligations are respected. Implementation of AI Systems should be well-designed and included in the pre-existing working model for predefined purposes. This dynamic planning prevents future problems, including copyrighted material in deliverables, lack of client consent or other non-compliance with applicable regulatory standards.

15. Intellectual Property

15.1 Applicability of Patent and Copyright Law

Even though most of the various intellectual property agencies' positions, as well as the classic academic doctrines, sustain that the centre of invention is "human" (anthropocentrism), the discussion continues with advances in generative AI.

Actions proposed by Dr. Thaler are the "classical" current decisions on this matter, which support the understanding (in the UK, USA, and some European jurisdictions) that AI Systems do not fulfil the requirements to be considered inventors or authors for the purposes of protection under IP rights (both patents and authorship rights). The future will tell if this position remains unchanged.

See also **8.1 Emerging Issues in Generative AI** and **8.2 IP and Generative AI**.

15.2 Applicability of Trade Secrecy and Similar Protection

Trade secrets, such as algorithms, datasets and proprietary AI models, play a crucial role in safeguarding AI innovations. Maintaining secrecy can be challenging, specifically in collaborative research environments or when AI technologies are integrated into shared products or services.

- Non-disclosure agreements (NDAs) are common and prevent unauthorised disclosure or use of AI-related confidential information by outlining the obligations of the parties involved in collaborations, research projects, or business partnerships, ensuring sensitive information remains confidential.
- Licensing agreements: to control the use of technology and data by third parties, protecting a company's IP rights under a commercial relationship.

In both cases, confidentiality can be compromised, and enforcement mechanisms are limited.

While contractual agreements offer valuable tools for protecting AI technologies and data, companies must adopt a comprehensive IP strategy, implementing robust contractual measures, balancing secrecy with collaboration and innovation.

15.3 AI-Generated Works of Art and Works of Authorship

The current dominant position relies on the anthropocentric nature of IP protection, which is applicable to artworks.

The emergence of AI-generated works of art has raised questions regarding authorship and related IP protection eligibility, as well as ownership of the copyright for AI-generated works.

In many jurisdictions, the default rule is that the human creator or the employer of the human creator owns the authorship rights to works created by an AI system. However, there is ongoing debate about whether AI itself should be recognised as the author and owner of its creations, particularly in cases where the AI System operates autonomously without direct human involvement in the creative process.

In addition to authorship rights, other forms of IP protection may apply to works generated by AI. Innovative AI algorithms or processes used to generate artistic or literary works could potentially be granted patents. Similarly, trademarks could protect distinctive logos, symbols, or brands associated with creative outputs generated by AI.

Overall, the changing landscape of IP protection for AI-generated works highlights the need for flexible and adaptive legal frameworks that balance innovation, creativity, and ownership rights in the digital age. As AI technologies continue to advance, policymakers, legal scholars, and stakeholders must collaborate to address the complex issues surrounding the protection and exploitation of AI-generated content in a manner that promotes both artistic expression and technological progress.

15.4 OpenAI

Pending IP litigation will undoubtedly dictate the industry. The cases pending on Open AI are the ones to keep an eye out for. One of the main points already mentioned is the IP issues raised by learning models (especially by web scrapping of publicly available information subject to copyright) and the "transformative" vs "reproductive" nature of the content generated by AI Systems. In addition to the rules and regulations that are emerging and are expected to regulate this issue in the future, one of the main arguments considered (with prominence in US case law) is the "fair use" test.

New trends are expected in case law, and companies are advised to pay close attention to these trends and adapt their business models to the new rulings and regulations.

16. Advising Corporate Boards of Directors

16.1 Advising Directors

Considering the overall absence of regulation as opposed to the several legal implications resulting from the use of AI, we recommend care and attention to this aspect from the beginning, ensuring compliance and good practices *"by design and default,"* namely by:

- Prioritise in-house, tailor-made AI Systems to guarantee data security in the training phase;
- Conduct comprehensive risk assessment tailored to the organisation's AI strategy, objectives, and industry context is crucial, identifying potential risks related to data privacy, security, compliance, ethics, reputation, client confidentiality and operational impacts;
- Ensure continuous alignment with relevant legal and regulatory requirements governing AI use, including data protection laws, industry-specific regulations and emerging AI guidelines;
- Establish robust governance frameworks and internal controls to govern AI development, deployment, and monitoring processes (defining roles and responsibilities, establishing clear policies and procedures, and implementing mechanisms for accountability, transparency, and ethical oversight).

Corporate boards should (i) engage with AI experts and advisors to stay informed about emerging AI trends, technologies and best practices; (ii) prioritise ongoing education and training on AI-related risks and opportunities for board members and senior executives; (iii) establish open channels of communication with stakeholders, including regulators, investors, customers, and employees, to address concerns and build trust, and (iv) incorporate AI risk management considerations into strategic decision-making processes to ensure alignment with business objectives and long-term sustainability.

17. AI Compliance

17.1 AI Best Practice Compliance Strategies

Implementing specific best practices for AI in organisations requires addressing several key issues, namely (in addition to the above):

- prioritise understanding the unique AI use cases, risks and opportunities. This involves conducting comprehensive AI impact assessments to identify potential ethical, legal, and technical issues;
- compliance with relevant applicable regulations;
- establish robust governance structures and processes to oversee AI development, deployment and monitoring;
- investment in building AI literacy and competency among employees to foster understanding, trust, and collaboration around AI technologies; and
- regularly evaluate and adapt AI best practices in response to evolving technologies, regulatory requirements and stakeholder expectations. Continuous monitoring, assessment and improvement of AI Systems and practices are essential to ensure ongoing compliance, effectiveness and relevance in a rapidly changing environment.

Trends and Developments

Contributed by:
Ana Rita Paínho and Ana Mira Cordeiro
Sérvulo & Associados

Sérvulo & Associados is a Portuguese full-service law firm with 20 years of existence, occupying a leading position in the Portuguese legal market. Widely recognised for the quality of its legal services in all relevant areas of law and strategic sectors, SÉRVULO has a highly competent multidisciplinary team of more than 100 lawyers, motivated by the purpose of transforming accumulated knowledge and experience in designing sound legal solutions in the benefit of its clients.

SERVULO'S TMT Team (with 8 members), led by Ana Rita Paínho, stands out in TMT. With practical and technical knowledge of the issues inherent to the technology industry, it provides legal and strategic advice on all relevant areas, including the software industry, e-commerce, the internet, and all matters related to new technologies, as well as regulatory issues in the telecommunications sector.

Authors

Ana Rita Paínho Head of the department, with more than 25 years of experience as a TMT specialist. Ana Rita assists on a broad spectrum of TMT matters, with particularly strong expertise in technology/IT (including IT contracts, software, internet and e-commerce), publicity and marketing and telecoms.

She acts for major names in the technology and telecommunications sectors and has considerable experience assisting international clients with local law issues. Ana Rita also handles TMT-related disputes.

Ana Mira Cordeiro Senior associate (top level), having over 24 years' experience in the fields of e-commerce and consumer protection, IP, TMTs, information society, software and Privacy and Personal Data Protection issues, and her activities have mainly focused on these fields. Apart from mainstream law firms and an in-house counsel to multinational companies and banks, Ana also worked with the national telecommunications regulator (ANACOM) for several years and, among other qualifications, has an LLM in International Trade and Business Law.

Sérvulo & Associados | Sociedade de Advogados, SP, RL

Rua Garrett
64 1200-204 Lisboa
Portugal

Tel: +351 21 093 30 00
Fax: +351 21 093 30 01/02
Email: geral@servulo.com
Web: www.servulo.com

Sérvulo & Associados | Sociedade de Advogados, SP, RL

General considerations – scope and reality

Artificial Intelligence (AI) has been the hottest topic in recent years, but even more in the past several months, being widely considered to be a (or "the") major groundbreaking science innovation, with the potential not only to change our daily lives but to impact humankind in ways that we are yet to anticipate or understand fully. But the interesting angle is that this is not science fiction anymore, as AI is not only being already widely and effectively used in modern societies in various contexts and with multiple applications, actively revolutionising industry and society worldwide, but is also notably impacting our daily lives, with applications and features that we are already accustomed to and even take for granted.

The baseline to understand this (r)evolution lies in the exact concept of IA (Intelligence Augmentation). Technicalities aside, AI is (just) a technology that enables computers and machines to simulate human reasoning, thought processes and problem-solving capabilities, thus simulating how the human brain works and, as such, human intelligence. AI is based on emulating human cognitive skills, such as learning, reasoning, self-correction and even creativity, having the capability to learn from existing data, innovate and frequently make more accurate classifications or predictions, constantly improving and "self-learning".

AI can be used individually or combined with additional technology (all sorts of machines, robots, cameras, sensors, etc) to execute tasks that usually require humans to perform or actively intervene. This makes it possible to free human resources from certain repetitive tasks and potentially allocate them to more creative ones.

Examples of AI uses are natural language processing, speech recognition, and machine vision, including certain widespread tools such as GPS, digital assistants, immediate translation features, autonomous vehicles, bots in customer service (where chatbots already fully replace human mediators along the customer journey) and generative AI tools (like Open AI's Chat GPT) which focus on generation of text, image and audio; all that have taken a comfortable place on our day to day.

The potential impact of AI is massive and continues to grow every day, not only in areas that are already being explored, such as automation of tasks, customer service work, quality control, all areas where AI can perform tasks much better than humans, faster and virtually free from errors, namely in repetitive, detail-oriented tasks, such as analysing large numbers of legal documents; but also in additional fields, such as pharmaceuticals development, robotics, learning tools and marketing, namely due to the massive volume of data that AI can process, analyse and relate almost instantly.

AI has already entered several markets, such as finance, banking, manufacturing, transportation, airport management, security, education, healthcare, weather forecasting, and law—to name a few—facilitating our daily lives in so many ways that we almost no longer have to think about them.

The advantages of welcoming AI into our lives are evident: reducing time and effort for heavy data analysis tasks, reducing risks of failure and human mistakes, particularly in detail-oriented tasks — increasing productivity in automated and low creativity tasks, improving customer satisfaction due to customisation based on past experiences and behavioural analysis, all by delivering consistent and reliable results and ensuring constant availability of resources (virtual assistants do not have working hours nor need breaks or PTO…). But needless to say, AI may also entail disadvantages, namely in regards to the need for specialised technical resources and lack thereof, with a limited supply of qualified workers, the need for an overall and comprehensive adaptation of the general workforce on the technical fields impacted, the potential elimination of human jobs and increased unemployment rates in less qualified sectors, current associated cost of the technology and initial investment, and an overall somewhat psychological resistance to determined features of the technology, among certain ranges of society.

In addition, AI brings to the discussion a whole new world of issues and challenges that require anticipation, analysis, and standings in various fields of discussion, namely the rethinking of how humans will and wish to live in an AI-powered society and the overall adaptation of society to the new reality, alongside the legal framework to accompany it and the impacting ethics considerations throughout.

Upcoming legal framework – the Artificial Intelligence Act

Despite AI's wide and progressive use and impact in modern society, little — if any — legal framework or, at least, strong guidelines issued by official national or international bodies or institutions exist.

In view of the overall impact and potential effects of AI, the recent enactment of the Artificial Intelligence Act (AIA) by the European Parliament (approved in March 2024 and expected to enter into force by late April 2024) marks the first major comprehensive high-level legislative effort towards AI regulation, which is expected to deepen from 2025 onwards, notably because EU companies or those wishing to operate in the EU market have one year to adapt to AIA.

As the first AI-specific legislation to be implemented in the world, AIA must be considered not only innovative but also real and groundbreaking landmark legislation in this field. It was, indeed, preceded by a complex discussion process, starting with the growing awareness of society and various stakeholders on AI's transformative potential and societal implications throughout the Union.

The European Commission's strategy focuses on building a digital Europe with the goal of achieving digital transformation by 2030, and it has been underscored by initiatives targeting digital skills, infrastructure, business transformation and innovation in public services. Aligned with other high-level legal instruments like the Data Governance Act, the Data Act, the Digital Services Act, and the Digital Markets Act, alongside the NIS/NIS2 Directive and the Cyber Resilience Act, the newly approved AIA, forms a cohesive legal framework, aimed at the said objective.

Being a Regulation, when enacted, the AIA will be immediately enforceable in all member states, which means that significant deviations will not be possible. Still, EU Regulations typically require additional implementation measures to ensure full compatibility within the national legal framework, which is expected to occur in the following months (or even a few years) following the entering into force. Nevertheless, a practical implementation may differ according to the political or social options of each Member State within the margins allowed by EU guidelines.

The key provisions of the AIA include:

- (i) harmonised rules for the placing on the market, putting into service and use of AI Systems;
- (ii) prohibitions of certain AI practices;
- (iii) specific requirements for high-risk AI Systems and obligations for operators of such systems;
- (iv) harmonised transparency rules for specific AI Systems;
- (v) harmonised rules for the placing on the market of general-purpose AI models;
- (vi) rules on market monitoring, market surveillance governance and enforcement; and
- (vii) measures to support innovation, focusing on SMEs and start-ups.

The AIA aims to improve the effectiveness of current rights and solutions by implementing specific requirements and duties. These include transparency, which entails providing users with comprehensive information about AI systems and their particular features, supplying and disclosing technical documentation, and keeping records of AI systems.

Notably, infringement of certain aspects of AIA is deemed an administrative offence, punishable with fines (to be determined on a case-by-case basis, considering the seriousness, duration, and consequences of the infringement and the size of the provider) that can be up to EUR35 million or 7% of total worldwide annual turnover for the preceding financial year, if the offender is an undertaking, in the most serious cases.

Although Portugal (along with other EU Members) has not yet enacted AI-specific legislation, and no specific national law/guidelines have been yet issued by competent NRAs, as an EU Member, it is bound to follow EU guidelines, and it is expected that Portugal abides by overall EU guidelines. However, considering the national interests as outlined in the AI Portugal 2030 strategy, Portugal may enact further solutions to oversight high-risk AI applications, potentially fostering a more favourable environment for certain types of AI development but still possibly assuming somewhat stricter positions in what regards to certain fields, such as health-related data management or analysis applications or under the scope of labour relationships.

Regulatory authorities have yet to be appointed, but the currently existing NRAs are expected to act as market surveillance authorities in their respective fields, as the AIA foresaw.

Challenges

As mentioned above, there's no denying that AI is already making significant strides across various industries, proving to be very beneficial, particularly in consumer-centric sectors like transportation and food delivery, where platform companies are at the forefront of the use and implementation of AI-based tools. Indeed, these AI systems are revolutionising customer experiences by providing personalised recommendations and tailored services. Moreover, the financial services sector (and the Portuguese market is also facing this issue) is undergoing profound transformations driven by AI systems, reshaping firm-client relationships and streamlining operations. Furthermore, AI is also revolutionising healthcare by integrating into patient treatment processes, monitoring health data on a large scale, and contributing to drug discovery efforts and diagnosing. The introduction of AI-powered autonomous vehicles has also revolutionised the automotive sector.

Nonetheless, AI also poses numerous challenges, particularly in terms of privacy and data protection law, consumer protection, cybersecurity, protection of IP-related rights, and overall liability, to name the frontrunners.

In regards to Privacy and Data Protection, AI (both generative and predictive) poses challenges arising from potential user misuse resulting from the nature of the learning models, as well as the possibility of perverse inversion attacks and data leakage. Indeed, compliance with all relevant GDPR principles presents significant challenges, as AI Systems require large amounts of (personal) data and may produce outputs that go beyond the original purpose of data collection. Only adequate regimes, strong data governance measures and tailored (by design and default) privacy-enhancing solutions to ensure compliance with GDPR and EU guidelines can tackle these issues. Companies are recommended to implement strict data governance and management practices, including transparent data collection, use and storage policies and robust mechanisms for obtaining and managing consent.

AIA particularly considers this issue, namely by mapping regarding data governance, aiming to ensure a good design phase and a development phase with due consideration from the GDPR regarding data collection, adequate data preparation, and precise measures to mitigate possible biases.

As for IP rights, generative AI holds major output on the legal issues raised, AIA focusing on the applicable standards for copyright protection due to the lack of a comprehensive range of legal solutions. This is particularly relevant to large language models (LLMs) concerning the use of copyrighted text and materials in training datasets. Different interests of developers, content owners and users are poorly regulated in the face of the new means of content creation, with various interpretations and potential legal gaps.

While the current norm and doctrinal standards lean towards an anthropocentric view of protection – sustaining that the centre of invention is and must continue to be "human" – the discussion continues with advances in generative AI, primarily applicable to art, once the emergence of AI-generated art raises questions concerning authorship, IP protection eligibility, and ownership of copyrights. Additionally, AI-generated works may require other IP protection tools, such as patents for innovative algorithms or trademarks for associated brands.

Notably, the protection of IP rights under AI and its assets, including models and training data used, input and output, depends, in addition to a strong and updated legal framework, on implementing vigorous and clear IP protection strategies by all interested parties, such as copyright registration and strong licensing agreements with tailor-made contractual provisions. The future T&Cs set by AI tool providers will play a significant role in determining the extent of IP rights and potential infringements.

Moreover, liability represents one of the major obstacles regarding the broad adoption of corporate AI. In the absence of specific national regulation, reference is made to two European-level projects: (i) amendments to the Product Liability Directive (PLD) and (ii) AI Directive (AILD), both still under discussion. Challenges include defining the scope, assessing defectiveness and fault, and ensuring proper disclosure of evidence. Active disclosure of adverse effects by generative AI producers is advisable.

Finally, additional ethical dilemmas surrounding generative AI also abound, including concerns about misinformation, privacy breaches, IP infringement, bias and discrimination, and the creation of false content, commonly referred to as “fake news.”

As generative AI continues to develop and become widely used, companies adopting it should ensure that they fully understand the risks associated with data collection and usage and take proactive measures to mitigate potential legal risks.

Hence, despite all the benefits AI provides, it is recommended that all corporate bodies engage with AI experts and advisors to stay informed about emerging AI trends, technologies and best practices. Also, companies should prioritise ongoing education and training on AI-related risks and opportunities for board members and senior executives, as well as establish open communication channels with stakeholders, including regulators, investors, customers and employees, to address concerns and build trust. Moreover, corporate bodies should incorporate AI risk management considerations into strategic decision-making processes to ensure alignment with business objectives and long-term sustainability.

Final remarks

All the above said on AI, applications, impacts, ethics and other considerations aside, one of the main issues concerning AI is that it not only is capable of “substituting” humans in the performance of certain (monotonous or repetitive tasks) – what’s new about this, right? However, it has the capability not only to be continuously instructed and taught to increase its capabilities and evolve but also to self-learn and self-improve as a result. And what can be considered as actually to “reason” and “think” as humans do (and what is “to think” other than problem-solving?), thus potentially becoming “intelligent” as we humans are, and just maybe, a little bit human also.

This thought alone is capable of breaking the barrier of what we consider to be human (as set apart from other animals): intelligence, learning, and creativity. What if the next step is self-awareness or consciousness? Ergo... life? But that’s another story and another Pandora’s box to be opened.