IP, DATA AND TECHNOLOGY

Legal matters:
2024 retrospective and outlook for 2025

Portugal and Spain

CUATRECASAS

May 2025

Contents

Editorial

The year 2024 was a transformation and adaptation milestone in major business areas, especially those involving emerging technologies and complex regulations. **Artificial intelligence ("AI")**, **cybersecurity, privacy and data protection, intellectual property**, **advertising and consumer law**, and **telecommunications** were at the center of important legislative and operational changes at both the European and national levels, with an emphasis on Spain and Portugal.

To ensure **safe, ethical and sustainable development**, the European Union ("EU") is implementing new legal frameworks and guidelines aimed at balancing technological innovation with the protection of citizens' fundamental rights.

As we move into 2025, companies face a regulatory transition marked by the enforcement of new rules and the continued need to adapt to evolving legal and technological requirements.

This guide provides a consolidated and practical overview of key trends and challenges, highlighting the importance of a proactive, multidisciplinary approach to ensure compliance, drive innovation and maintain competitiveness in Iberian and European markets.

Legal framework

	Artificial intelligence	Intellectual property	Privacy and data protection	Telecommunications and technology	Cybersecurity	Advertising and consumer law
LEGISLATION IN FORCE SINCE 2024	AI Act	New European legislative package for designs	Access to Metadata Act	Media Freedom Act	Supplementary delegated regulations to the DORA Regulation Rules for applying the NIS2 Directive Cyber Resilience Act	Digital Services Act Product Liability Directive Ecodesign Requirements for Sustainable Products Act Green Transition Directive Directive Promoting the Repair of Goods
FORTHCOMING LEGISLATION AND DEVELOPMENT PLANS	Spanish preliminary draft law on AI regulation EU InvestAI AI Continent Action Plan		Regulation on the European Health Data Space, procedural rules relating to the GDPR		Transposition of the NIS2 Directive Cyber Solidarity Act EU Cybersecurity Act revision Cybersecurity Blueprint	Transposition of the Directive Promoting the Repair of Goods Transposition of the Directive on Empowering Consumers for the Green Transition

Artificial intelligence

With the entry into force of **Regulation (EU) 2024/1689** of June 13, 2024 ("AI Act") and the establishment of the **European Artificial Intelligence Office**, Europe has strengthened its position as a global leader in regulating AI systems. Also, the **Artificial Intelligence Treaty** and the **specific Recommendations of the European Data Protection Supervisor** ("EDPS") and of the OECD for data protection in AI systems have become fundamental guides for public and private sector companies.

As we move ahead in 2025, the forecasts point to a year of regulatory transition and growing adoption of AI in strategic sectors. The **partial** applicability of the AI Act will mark the first steps in the practical implementation of the new rules.

On February 11, 2025, the EU launched the **InvestAI** initiative to mobilize €200 billion for AI investment, including a €20 billion fund for AI gigafactories. Similarly, the **AI Continent Action Plan**, presented on April 9, 2025, outlines strategies to enhance AI infrastructure, talent and adoption throughout Europe.

Artificial intelligence | EU legislation

Artificial Intelligence Regulation or AI Act

The pioneering EU AI Act is crucial for businesses, as it establishes a common risk-based framework and imposes a broad set of obligations on all those involved in the AI value chain, from providers to deployers.

It also introduces substantial penalties for cases of non-compliance, as highlighted below. Consequently, organizations must identify and mitigate the risks associated with their AI models through specific measures.

See our Guide: *AI Act: Practical Guide*

August 2, 2024	February 2, 2025	August 2, 2025	August 2, 2026	August 2, 2027
Entry into force	Application of the general provisions of the AI Act, literacy requirements, and prohibited AI practices (Chapters I and II)	Provision of general-purpose AI systems and raising awareness of the relevant new regulatory and supervisory bodies (Chapter III, section 4, Chapter V, VII and XII and article 78, except for article 101)	General application of the AI Act, except for the classification and corresponding obligations of high-risk AI systems	General application of the AI Act, with no exceptions

Non-compliance (maximum limits)

- €35 million or 7% of annual turnover (whichever is higher) for prohibited AI practices
- €15 million or 3% for breaching other obligations
- €7.5 million or 1% for providing incorrect information
- For small and medium-sized enterprises ("SMEs"), including startups, the fines may not exceed the lower of these amounts and percentages.

ACTION POINTS

- Assess the impact of the AI Act
- Map the AI systems used/developed
- Classify the AI systems and assess the inherent risks
- Establish an action plan with possible mitigation measures to be implemented
- Create an internal management system to govern the use of AI in an organization
- Raise awareness and provide training for AI system users (promoting AI literacy)

Artificial intelligence | Spanish legislation

Spain – Preliminary draft law on artificial intelligence

In March 2024, Spain introduced its preliminary draft law on artificial Intelligence to complement the EU AI Act at the national level.

The proposal includes:

- establishing a **national AI supervision system**, led by the Spanish Agency for the Supervision of AI (AESIA);
- **requiring mandatory labelling** of AI-generated content, such as images, video and audio;
- implementing rules on **algorithmic transparency**, **impact assessments** and **redress mechanisms**; and
- creating a framework for **regulatory sandboxes** to test and validate AI systems under supervision.

The law is currently under public consultation and is expected to align with the full entry into force of the AI Act.

See our Post: *Anteproyecto de Ley para el buen uso y gobernanza de la IA*

KEY POINTS - sanctioning regime summary

The draft law specifies the applicable sanctioning regime, categorizing infringements as minor, serious or very serious, each linked to corresponding penalties.

- **Very serious infringements** incur fines between €7.5 million to €35 million, or 2% to 3% of the global turnover from the preceding year, whichever is higher. For SMEs, the lower amount applies. For very serious infringements involving prohibited AI practices or where an AI system has caused a serious incident, the market surveillance authority may order product withdrawal, system disconnection or prohibition of the AI system.
- **Serious infringements** incur fines between €500,000 and €7.5 million, or 1% to 2% of global turnover, whichever is higher. For SMEs, the lower amount applies.
- **Minor infringements** incur fines between €6,000 and €500,000, or 0.5% to 1% of global turnover, whichever is higher. For SMEs, the lower amount applies.
- The law establishes criteria for determining the severity of sanctions, prioritizing impacts on health, safety and fundamental rights.
- Regardless of the sanction imposed, offenders must restore the original situation and compensate for any damage caused, as determined by the competent authority.
- To ensure the sanction is effective, the competent authorities may impose precautionary measures, including temporary withdrawal, disconnection or prohibition of the AI system, should its continued operation pose an unacceptable risk during proceedings.

Artificial intelligence | EU (EDPS) guidelines

European Data Protection Supervisor (EDPS) guidelines - Generative AI systems

Provides guidelines for the EU institutions, bodies, offices and agencies ("EUIs") to ensure compliance with data protection obligations when using generative AI systems.

Highlights the importance of principles such as **data minimization**, **accuracy and transparency,** and the need for data protection impact assessments ("DPIAs") for high-risk AI systems.

Emphasizes the responsibility of EUIs to develop and use AI **ethically and legally**, avoiding bias and ensuring data security. Generative AI systems present challenges for protecting personal data and transparency for individuals. EUIs must adopt a **robust data governance policy** and involve data protection officers at every phase of the AI systems' lifecycle to ensure regulatory compliance.

See our Post: *EDPS guidelines on the use of generative AI*

ACTION POINTS

- Ensure that the data protection officer is involved in the use of AI systems processing personal data
- Ensure compliance in developing and implementing a generative AI system with data protection obligations
- Identify and understand the life cycle and functioning of AI systems, particularly to ensure the identification of the origin/source of personal data, and the legal basis for processing
- Understand the results generated by AI systems (how the input and output mechanisms work) and analyze the decision-making processes implemented in the system
- Apply data protection principles
- Ensure compliance with data protection procedures, in particular: (i) conducting a data protection impact assessment, where applicable; (ii) updating the register of processing activities; and (iii) ensuring the review and conclusion of data processing agreements

Artificial intelligence | EU (EDPB) guidelines

EDPB: Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models

The Irish supervisory authority asked the European Data Protection Board ("EDPB") for an opinion on the **application of the GDPR in the development of AI models**, addressing anonymization, legitimate interest and unlawful processing of personal data.

In its opinion, the EDPB:

- stressed the need for case-by-case assessments for anonymization;
- said that a three-step test should be conducted to justify legitimate interest and consideration of data subjects' expectations;
- presented three unlawful processing scenarios, each requiring a specific GDPR compliance assessment; and
- emphasized the importance of mitigation measures and data protection compliance.

ACTION POINTS

- Document the anonymization process in detail and keep records that prove the anonymity of the data used in AI systems
- Conduct legitimate interest assessments and DPIAs to analyze the impact of processing on data subjects
- Consider data subjects' reasonable expectations when developing and implementing AI models
- Establish procedures to deal with unlawful data processing scenarios, including data retention in AI systems, processing by another controller, and anonymization before further processing

Artificial intelligence | EU (EDPB) guidelines

EDPB Report – AI Privacy Risks & Mitigations Large Language Models (LLMs)

In April 2025, the EDPB published a report providing guidance on managing privacy risks associated with AI systems built on large language models ("LLMs").

The report highlights that LLMs may inadvertently process personal data during training and deployment, raising data protection concerns. It stresses the need for providers and deployers to conduct thorough risk assessments and establish safeguards to mitigate potential privacy risks.

The report outlines a practical approach toward managing risks throughout the lifecycle of LLM systems, covering:

- inception and design;
- data preparation and pre-processing;
- deployment and model training;
- verification and validation;
- operation and monitoring;
- re-evaluation, maintenance and updates; and
- retirement.

Therefore, it identifies risks such as exposure of sensitive data, data bias and insufficient safeguards. The report also includes real-world examples of applying a risk management framework, such as virtual assistants and chatbots for customer queries, systems monitoring and supporting student progress, and AI assistants for travel and schedule management.

ACTION POINTS

- Carry out risk assessments and specific data protection impact assessments for LLMs, including algorithmic audits
- Draft or review internal policies and risk mitigation procedures
- Adopt internal AI compliance programs for LLMs

Artificial intelligence | OECD guidelines

OECD Recommendation – AI

The OECD has updated its Recommendation on AI to guide member countries in creating policies that promote responsible AI development. It highlights the following:

- Importance of transparency, explainability, protection of human rights, and promotion of inclusive and sustainable AI
- Human-centered approach, ensuring robustness and security of AI systems, and high-quality data governance
- Accountability of providers and those responsible for implementing AI systems
- International cooperation to tackle global challenges by sharing best practices and collaborating on research and development.

View our Post: *OECD updates AI principles*

ACTION POINTS

- Develop and implement transparent and explainable AI systems
- Conduct impact assessments of ethical and fundamental rights to identify and mitigate possible AI system risks
- Adopt practices that promote inclusion and sustainability in the use of AI
- Ensure that AI systems are robust and secure against attacks and security breaches
- Create clear accountability mechanisms for AI system developers and operators
- Use high-quality data and protect them from misuse
- Promote international cooperation by sharing good practices and collaborating on research and development

Artificial intelligence | EU Commission guidelines

European Commission guidelines – Definition of AI system

On February 6, 2025, the European Commission published guidelines to clarify the scope of the term **"AI system"** as defined in **Article 3.1** of the AI Act. These guidelines aim to ensure consistent classification and provide legal certainty for developers, deployers and regulators.

The guidelines detail the structural and functional elements required for a system to be considered AI under the AI Act. According to the Commission's guidance, an AI system:

- is a **machine-based system** that is designed to operate with varying levels of autonomy;
- is designed to achieve **explicit or implicit goals** set by humans;
- **infers outputs** (e.g., predictions, recommendations, decisions, or content) from input data;
- may employ various techniques, including **logic-based, statistical or machine-learning approaches**; and
- may modify or adapt its behavior **with or without human intervention** following deployment.

This definition is broad and **technology-neutral**, covering both simple rule-based systems and complex models, such as deep neural networks. Although not all elements need to always be present, inference capability is a key criterion.

View our post: *"AI system" definition guidelines*

ACTION POINTS

- Evaluate whether the system processes data to generate autonomous or semi-autonomous outputs
- Identify the techniques used, such as symbolic AI, machine learning (ML), or Bayesian inference, and assess its inference capabilities
- Determine whether the system's behavior can evolve over time in response to input data or environmental changes
- Apply the AI system definition consistently across all lifecycle stages (development, deployment and updates)
- Maintain documentation that justifies classification decisions and ensures traceability

Artificial intelligence | EU Commission guidelines

European Commission guidelines – Prohibited AI practices

In February 2025, the European Commission published guidelines to clarify the interpretation and enforcement of **Article 5 of the AI Act,** which prohibits specific AI practices considered to pose unacceptable risks to fundamental rights.

The guidelines outline the types of systems strictly prohibited under EU law and provide examples to ensure consistent application by providers, users and authorities. These prohibited practices include:

- using subliminal or manipulative techniques that may cause harm;
- exploiting vulnerabilities, such as age or disability, to influence behavior;
- deploying social scoring systems based on personal or behavioral traits;
- conducting predictive profiling for criminal risk without objective and verifiable evidence;
- scraping facial images indiscriminately to build biometric databases;
- using emotion recognition systems in workplaces or educational settings (except for health and safety reasons);
- employing biometric categorization systems to infer sensitive attributes like race or political beliefs; and
- performing real-time remote biometric identification in public spaces by law enforcement (subject to limited exceptions).

See our post: *Prohibited AI Practices Guidelines*

ACTION POINTS

- Identify system features that may constitute prohibited categories under Article 5 of the AI Act
- Assess use cases involving biometric recognition, profiling, emotion detection, or behavioral targeting
- Implement internal controls to detect and prevent the deployment of prohibited functionalities
- Refrain from unjustified data scraping or the use of biometric data for categorization or scoring purposes
- Have document compliance justifications for borderline cases and submit them for consultation when necessary

Artificial intelligence | EU Commission model clauses

European Comission – Updated model contractual clauses for AI procurement

On March 5, 2025, the European Commission published an updated version of its model contractual clauses for responsible AI procurement ("MCC-AI"). These clauses aim to assist public sector organizations procuring AI systems developed—or to be developed—by external suppliers.

The MCC-AI include standardized contractual provisions tailored to AI, aligning closely with obligations and requirements for high-risk AI systems as outlined in Chapter III of the AI Act. The updated MCC-AI contain detailed provisions that address both high-risk and non-high-risk AI systems, along with a comprehensive commentary that offers practical guidance on when and how to apply the clauses effectively.

For high-risk AI systems, the MCC-AI primarily provide contractual safeguards that ensure public authorities comply with their legal obligations under the AI Act. Key provisions cover:

- risk management frameworks;
- data handling, governance and rights of use;
- technical documentation, instructions and record-keeping;
- transparency and oversight mechanisms, including AI system registries;
- accuracy, robustness and cybersecurity requirements; and
- annexes with practical templates to facilitate implementation for public buyers and suppliers.

For non-high-risk AI systems under the AI Act that may still pose significant risks (especially those involving general-purpose AI models), the MCC-AI offer tailored clauses that public buyers can adopt as a precautionary measure to safeguard health, safety and fundamental rights.

Although primarily designed for public sector entities, the MCC-AI reflect best practices applicable to private organizations, too. Therefore, they can be used to update procurement contracts, ensuring that both public and private entities comply with the AI Act.

ACTION POINTS

- Audit current AI procurement contracts to identify gaps in alignment with MCC-AI standards
- Incorporate MCC-AI clauses in upcoming tenders by integrating the standardized MCC-AI clauses—tailored to either high-risk or non-high-risk systems—into procurement templates and tender documentation
- Use the practical templates provided in the MCC-AI annexes to simplify contract drafting, supplier evaluation and post-deployment monitoring of AI system performance
- Provide targeted training for procurement officials and legal advisors on applying the MCC-AI and its interplay with the AI Act

Artificial intelligence | 2025 forecast

01

Partial applicability of the AI Act

The year 2025 marks the beginning of the application of the AI Act.

From February 2, companies must guarantee the following:

- **AI training and literacy**: The persons involved in operating and using AI systems must have a sufficient level of AI literacy.
- **Prohibited AI practices**: Discontinuation of the use of AI systems, particularly prohibited AI practices.
- Inventory system.

In August, the focus will be on **general-purpose AI models.** To this end, from August 2, providers of these models will have to ensure the following:

- **Compliance**: Compliance with various obligations relating to technical documentation, transparency and making information available, which must be recorded in internal policies and other publicly accessible documents.
- **General-purpose AI models with systemic risk:** Providers of these AI models will have to notify the Commission and comply with additional obligations, including technical assessment, model testing documentation, incident reporting to competent authorities, and ensuring appropriate cybersecurity levels.

By that date, each Member State must also have designated or established **competent regulatory and supervisory bodies.**

02

AI Liability Directive proposal (WITHDRAWN)

In 2022, the European Commission presented the proposal for the **AI Liability Directive**, aimed at aligning private law with the digital economy transition requirements and making it easier to bring claims for damage caused by AI systems and the use of AI.

However, in February 2025, the European Commission announced in its 2025 Work Programme that it would withdraw the proposal, citing the lack of a foreseeable agreement between co-legislators.

The directive was meant to complement the AI Act and establish a unified framework for civil liability related to AI. However, the Commission concluded that recent reforms to the Product Liability Directive, combined with the entry into force of the AI Act, currently provide sufficient legal coverage.

The withdrawal of the AI Liability Directive leaves unresolved how liability should be allocated in cases involving autonomous and opaque AI systems, particularly when causation is complex or cannot be clearly traced to a human actor or product defect. Consequently, there remains no harmonized EU framework to address damage caused by AI behavior that falls outside traditional liability models. In the current legal system, these cases will continue to fall under national tort law, increasing the risk of regulatory fragmentation for individuals across Member States.

Artificial intelligence | 2025 forecast

03

EU InvestAI

On February 11, 2025,the EU launched the **InvestAI** initiative to mobilize €200 billion in AI investment across Europe. This includes a €20 billion fund to finance up to five **AI gigafactories**, which will provide the **large-scale computing infrastructure** needed to train and develop advanced AI models.

Designed as **a public–private partnership**, InvestAI supports not only major industry players but also startups and SMEs, ensuring broad access to cutting-edge AI resources.

The initiative leverages existing **EU funding programs**, such as **Digital Europe** and **Horizon Europe**, while encouraging additional contributions from Member States.

By reducing investment risk and pooling resources, InvestAI aims to:

- accelerate trustworthy AI development;
- foster open innovation; and
- strengthen Europe's global competitiveness in strategic sectors like healthcare, manufacturing and biotechnology.

04

AI Continent Action Plan

Presented on April 9, 2025, the **AI Continent Action Plan** (the "Action Plan") sets out the European Commission's strategy to establish the EU as a global leader in AI.

The plan focuses on five key areas:

1. Building a large-scale **AI computing infrastructure**
2. Increasing access to **high-quality data**
3. Promoting **AI adoption in strategic sectors**
4. Strengthening **AI skills and talent**
5. **Simplifying the implementation of the AI Act**

Central to the plan is the creation of at least 13 AI factories and up to 5 gigafactories, leveraging Europe's supercomputing network to support startups, industry and research.

The Action Plan also introduces measures to boost private investment in cloud and data centers, foster a single market for data and launch the "Apply AI" strategy to drive AI uptake in both public and private sectors.

Intellectual property

The year 2024 was marked by legislative developments in the field of intellectual property in the EU. These included the adoption of the legislative package comprising **Regulation (EU) 2024/2822** and **Directive (EU) 2024/2823**, aimed at **modernizing and simplifying the industrial design protection system.**

Moreover, the European Commission's Recommendation (EU) 2024/915 of March 19, 2024, established **measures to combat counterfeiting** and enhance the enforcement of intellectual property rights in the EU.

Court decisions on intellectual property include the judgments of the Court of Justice of the European Union ("CJEU"), which **clarified the scope of application and protection of copyright, trademark and patent rights**, tackling issues such as the referential use of trademarks, the burden of proof for certain cases, the protection of applied art works, and the modification of computer programs.

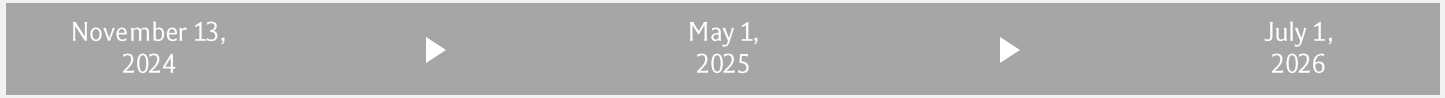
Intellectual property | EU legislation

New European legislative package for designs

The legislative package comprising Regulation (EU) 2024/2822 and Directive (EU) 2024/2823 aims to modernize and simplify the **industrial design protection system in the EU**, harmonizing registration rules and introducing quicker and less bureaucratic procedures. The reform facilitates the **registration** process, **reduces costs**, combats **piracy** and **counterfeiting**, and strengthens **holders' rights**. It also extends the **protection of unregistered designs** and adapts the legislation to new technologies, such as digitization and 3D printing, ensuring effective protection in the digital environment.

View our post: *Reform of European design legislation published*

Regulation (EU) 2024/2822



Entry into force

Application of the regulation, with some exceptions regarding the proposed changes to Regulation 6/2002 of December 12

(Articles 1.21, 1.22, 1.24, and 1.26 to articles 1.30, 1.32.b), 1.34.b), 1.37, 1.40, 1.42, 1.45, 1.46, 1.49, 1.52, 1.54, 1.56, 1.58, 1.61, 1.63, 1.65, 1.66, 1.70, 1.72, 1.74, 1.76, 1.78, 1.80.b), 1.81, 1.85, and 1.88, insofar as it concerns articles 72.3.a), 72.3.e), 72.3.f), and 72.3.m), and articles 90, 98.b), 111, 113, and 123).

General application of the regulation

Directive (EU) 2024/2823

Entry into force and date of application of the Directive, with some exceptions regarding the substantive law on designs (Articles 4, 5, 7, 8, 9, 20 and 22)

General application of the Directive

ACTION POINTS

- Companies must ensure that their design registration procedures comply with the **new requirements established by Regulation (EU) 2024/2822 and Directive 2024/2823**.
- Companies must take proactive measures to protect their designs against counterfeiting. This includes **monitoring the entry of products into the EU market** and using the **customs procedures** established in Regulation (EU) 608/2013 to prevent the entry of products that infringe their design rights.
- Companies that manufacture or sell components of complex products must clearly inform consumers of the commercial origin and the identity of the manufacturer of the products used for repairs to comply with the "**repair clause**" and avoid legal issues.

Intellectual property | Commission recommendation

Commission Recommendation - Combating counterfeiting and improving respect for IP rights

European Commission Recommendation (EU) 2024/915 of March 19, 2024, establishes measures to combat counterfeiting and enhance the enforcement of intellectual property rights in the EU by:

- highlighting the need for a robust policy against these illegal activities;
- promoting cooperation between rights holders, intermediary service providers, and competent authorities, and encouraging the use of new technologies and good practices;
- promoting the modernization of voluntary instruments, the designation of single points of contact, and the use of tools such as the IPR Enforcement Portal (IPEP) and the Safety Gate early warning system;
- establishing specific measures to prevent the misuse of transportation, logistics, payment, and social networking services;
- promoting alternative dispute resolution;
- promoting adaptation to new technologies such as AI; and
- encouraging intellectual property awareness-raising and training, especially for SMEs, through initiatives such as the SME Fund and cyber theft prevention tools, underscoring the importance of a coordinated and collaborative approach to protecting innovation and investment in the EU.

ACTION POINTS

- Establish partnerships and collaborate closely with rights holders, intermediary service providers, and competent authorities to combat counterfeiting and piracy, including through the use of voluntary instruments such as memoranda of understanding
- Designate **single points of contact within the company** to deal with issues of respect for intellectual property rights
- Adopt and **implement new technologies**, such as AI and advanced tracking systems, to **identify and combat counterfeit goods**
- Use tools such as the **IPR Enforcement Portal** (IPEP) and the **Safety Gate rapid alert system** to facilitate cooperation and the sharing of information about illegal activities

Intellectual property | Caselaw

Trademark infringment

The judgment of the CJEU of January 11, 2024 in Case C-361/22 interpreted article 6.1.c) of Directive 2008/95/EC, which allows the **use of trademarks by third parties** to indicate the destination of products or services, provided it is in accordance with honest practices.

The dispute in the main proceedings saw Inditex and Buongiorno Myalert at odds over the use of the "ZARA" trademark in an advertising campaign, with the court concluding that this **use is only permitted when necessary to indicate the destination of a product or service offered by the third party**.

Exhaustion of rights conferred by an EU trademark

Judgment C-367/21 of the CJEU of January 18, 2024, addresses the exhaustion of trademark rights in the case between Hewlett Packard and Senetic. The court decided that the burden of **proof regarding the exhaustion of trademark rights cannot fall solely on the plaintiff**, especially when the products do not clearly identify the destination market and are distributed by selective networks.

In these cases, the trademark owner must prove that the products were initially placed on the market outside the EEA to avoid compartmentalization of the national markets and ensure the free movement of products, balancing the protection of intellectual property rights with internal market freedoms.

Copyright infringement

Case C-159/23 concerns a reference for a preliminary ruling in which the CJEU was asked whether the modification of the content of variables stored in the internal memory of a computer by another program, without altering the source code or object code of the protected program, constitutes a copyright infringement under Directive 2009/24/EC. The CJEU concluded that **the protection granted by the directive only applies to the literal expression of the computer program, such as the source code and object code, and not to the underlying ideas, principles or functionalities**. Therefore, the modification of the content of variables by another program that does not allow the reproduction or subsequent realization of the protected program is not covered by the directive's protection.

Intellectual property | Caselaw

Copyright Infringement

In Case C-227/23, the CJEU was asked to interpret the **applicability of copyright on works of art specifically applied in the context of the Berne Convention and Directive 2001/29/EC**. The court concluded that Member States cannot apply the Berne Convention's criterion of material reciprocity to works from third countries, and that the copyright harmonization must be determined by EU legislators.

This decision ensures standard and high protection for all works in the EU internal market, regardless of the author's country of origin or nationality.

Deadline for claiming the priority right in design and patent registration

Judgment C-382/21 of the CJEU of February 27, 2024, addressed **applying the six-month priority period of Article 41 of Regulation (EC) 6/2002 to international patent applications**.

The dispute in the main proceedings involved The KaiKai Company Jaeger Wichmann GbR, which claimed priority based on an international patent application under the Patent Cooperation Treaty. The **General Court held that there was a legal loophole and applied the 12-month time limit of the Paris Convention**.

However, the CJEU disagreed, stating that Article 41 clearly and exhaustively limits the right of priority to six months for design applications, and concluded that the General Court's decision exceeded the limits of a conforming interpretation.

Suspension of infringement proceedings due to pending EUIPO invalidity action – Spain

The Spanish Supreme Court, in judgment 78/2025 (January 14, 2025), reinterprets Article 132.1 of Regulation (EU) 2017/1001. Specifically, it holds that national courts must **stay EU trademark infringement proceedings** when a parallel invalidity or revocation action is pending before the EUIPO, **even if filed after the judicial claim**.

This marks a departure from earlier caselaw, which required the EUIPO procedure to be pre-existing. The judgment introduces a **mandatory suspension mechanism** that restricts judicial discretion, altering procedural strategies in EU trademark enforcement. Courts may only avoid the stay if they find **special grounds** to proceed, making the judgment a **pivotal change in Spanish litigation practice**.

Although controversial, the decision is binding and is expected to **reshape procedural tactics in infringement cases involving EU trademarks in Spain**, at least until the CJEU revisits or clarifies the judgment.

Intellectual property | 2025 forecast

01

Unified Patent Court

The expected referendum in Ireland on ratifying the Unified Patent Court Agreement may take place, which would bring Irish companies under the UPC's jurisdiction.

This change would enable the centralized enforcement of European patents, simplifying litigation for patent holders.

However, it could also raise questions about jurisdictional changes and practical implications for companies operating in Ireland.

02

Protection of AI-related intellectual property

With the continuing advance of AI tools, legal debates on the protection of AI-generated works and the patentability of inventions driven by these technologies are likely to intensify. Fundamental issues such as protecting AI-generated creations under intellectual property law and whether the use of third-party intellectual property to train AI models constitutes an infringement will be at the center of the discussions. At the same time, topics such as the role of human inventors, novelty and inventive step criteria, and the potential consideration of AI as an inventor in its own right could lead to legislative changes or the development of new caselaw.

Both in the EU and worldwide, these changes are expected to bring greater clarity and definition to the legal framework for addressing these issues in 2025, mainly at a caselaw level and with the applicability of some of the provisions of the AI Regulation from February of this year.

Companies innovating in the field of AI must carefully monitor these developments, ensuring that their creations and inventions are properly protected and comply with the emerging standards.

See Artificial intelligence section.

Privacy and data protection

In 2024, there was a consolidation of concepts and methods for collecting and processing personal data, especially the guidelines issued by the EDPB on the use of **facial recognition technologies**, the Spanish Data Protection Authority ("AEPD") on the risks of **Wi-Fi tracking**, as well as the rulings of the CJEU **on the principles enshrined in the GDPR** and the **calculation of** applicable **fines**.

Extraordinary fines were **imposed** throughout Europe in 2024, most notably the €310 million fine imposed on LinkedIn by the Irish Supervisory Authority.

It should also be noted that the Portuguese Supervisory Authority ("CNPD") investigated and subsequently suspended **biometric data processing** by the Worldcoin Foundation, whose project aimed to create a digital proof of identity (WorldID).

The year 2025 will certainly be no different for existing data protection dynamics, specifically regarding the decisions of competent administrative and judicial authorities, the organization of business structures, and the attention given by data subjects to these issues.

Privacy and data protection | EU guidelines

Valid consent in the context of implemented consent or payment models by large online platforms

The Supervisory Authorities of the Netherlands, Norway and Germany have asked the EDPB for an opinion on the conditions under which **large online platforms** can validly and freely apply "**consent or pay**" models for **behavioral advertising**. The EDPB stresses the following:

- Consent must comply with the GDPR principles, including those of necessity, proportionality and fairness. Platforms must ensure the availability of alternatives that are free or involve less processing of personal data.
- Consent must be freely given, without the imposition of a fee that compromises the data subjects' freedom of choice, especially when the service is essential to social or professional life.
- Conditional consent must be avoided, and equivalent alternatives that do not require the processing of personal data must be offered.
- Consent must be specific, informed and explicit, enabling for granularity in the stated purposes. Those responsible must avoid misleading models, assess the frequency of consent renewal, facilitate its withdrawal, and ensure that data subjects fully understand their choices and the associated consequences.

ACTION POINTS

- Provide clear and comprehensible information regarding the options available to data subjects in a Consent or Pay model so that they can make a truly free choice
- Ensure that the consent collected is free, specific, informed, and explicit
- Ensure that the fee required in the payment model is not so high as to condition the data subject's choice.

Privacy and data protection | Spain guidelines

Guidance on the risks of Wi-Fi tracking

The guidelines prepared by the Spanish authorities (AEPD, APDCAT, AVPD and CTDPA) on the risks of Wi-Fi tracking highlight rising concerns about privacy and personal data protection. These guidelines stress the importance of full transparency and informed consent from individuals whose devices may be monitored through these technologies. They also emphasize that deploying these systems must be legally and ethically justified, as well as technically sound.

- **Organizations must clearly define and communicate legitimate, specific purposes** for using Wi-Fi tracking, avoiding vague or excessively broad justifications. Also, all actions must comply with GDPR principles of purpose limitation and data minimization.
- **The design and deployment of tracking systems must adhere to a privacy-by-design and by-default approach**, ensuring that safeguards are not merely retrofitted but are embedded from the outset. This includes limits on data retention, granularity and spatial coverage.
- **Data controllers are expected to assess whether** Wi-Fi tracking is necessary and proportionate when compared to less intrusive alternatives. A system's technical feasibility does not inherently justify its legal or ethical acceptability.
- **DPIAs should be carried out systematically** and not treated as a mere formality. Rather, DPIAs should function as rigorous risk-management tools, especially where tracking could lead to profiling or behavioral inference.
- **Robust security measures, including encryption, access control and regular auditing, must be implemented** to prevent unauthorized access, data breaches and misuse of location-based data.
- **Authorities are urged to enforce compliance proactively**. They should move beyond reactive complaint-handling, instead promoting accountability mechanisms such as independent audits, transparency reporting and sector-specific guidance.
- **Companies should resist the silent normalization of surveillance**, especially in public or semi-public spaces, where individuals have a legitimate expectation of freedom of movement without being unknowingly monitored.

ACTION POINTS

- Clearly inform data subjects about the collection of data through Wi-Fi tracking
- Obtain data subjects' free, specific, informed, and explicit consent before collecting their data
- Implement and review advanced security measures to protect the collected data from unauthorized access and security incidents
- Conduct DPIAs to identify and mitigate risks associated with Wi-Fi tracking
- Offer data subjects a clear and easy option to reject the collection of their data through Wi-Fi tracking

Privacy and data protection | EU (EDPB) guidelines

Guidelines 2/2023 on the technical scope of Article 5.3 of the ePrivacy Directive

The EDPB Guidelines, adopted on October 7, 2024, clarify the application of Article 5.3 of Directive (EU) 2002/58/EC ("**ePrivacy Directive**") to various technical solutions, addressing ambiguities related to new tracking tools.

The guidelines aim to **protect the private sphere of users**, covering not only personal data but also any information stored on terminal equipment. The protection applies to operations that involve storing or accessing information on the terminal equipment of a subscriber or user, regardless of the origin or nature of the information.

Article 5.3 of the ePrivacy Directive is not restricted to the use of cookies, but also to similar technologies.

The guidelines identify and analyze the main elements associated with the article under analysis: **"information," "terminal equipment of a subscriber or user," "public communications network," "gaining access,"** and **"stored information."**

ACTION POINTS

- Ensure that any use of tracking technologies, such as cookies, device fingerprinting and pixels, is preceded by obtaining the data subjects' explicit and informed consent
- Adopt measures to protect data subjects' privacy, ensuring that any access to or storage of information on terminal equipment is regulated and has their consent

Privacy and data protection | EU caselaw

Interpretation of the concept of "personal data"

Case C-604/22 examined the definition of "personal data" and the responsibility of sectoral organizations in processing consent-related data in digital advertising.

The CJEU concluded that the transparency and consent string (TC String) used by IAB Europe in the transparency and consent framework (TCF) **constitutes personal data, as it is capable of identifying individuals**.

IAB Europe was considered a "joint controller" of personal data, as it influences the purposes and means of processing, even without having direct access to the data in question.

However, the CJEU clarified that its liability does not automatically extend to future processing performed by third parties such as website providers, unless the IAB directly influences that processing.

Access to personal data in a criminal investigation without judicial authorization

Case C-548/21 of the CJEU addressed the **legality of the seizure and access to cell phone data by police authorities without judicial authorization** in criminal investigations.

The CJEU concluded that this access constitutes a serious interference with the rights to privacy and protection of personal data and **must be limited to investigations into serious criminal offenses and subject to prior review** by a judge or independent body, except in cases of justified urgency.

The national legislation in question, which allows access without judicial authorization, is incompatible with Directive (EU) 2016/680 and the Charter of Fundamental Rights. In particular, the authorities must inform data subjects of the attempted access unless that information compromises the investigation.

Likewise, the regulations must clearly define the infringements that justify this access, respecting the principle of proportionality.

Privacy and data protection | Supervisory authority decisions

General data protection principles

Amazon France Logistique, responsible for Amazon's warehouses in France, was investigated by the French Supervisory Authority ("CNIL") following complaints about the **use of scanners to monitor employees' activity in real time.**

The CNIL identified several irregularities, including the breach of the principle of data minimization, excessive and illegal use of productivity indicators, lack of adequate information for temporary employees and visitors about data collection and video surveillance, and security breaches in access to video surveillance software.

The decision highlighted the need to respect the principle of data minimization, ensure transparency and security in personal data processing, and avoid excessive control of employees.

ACTION POINTS

- Ensure that employee monitoring practices are proportionate and justified, avoiding excessive control and respecting employees' privacy rights
- Clearly inform all temporary and permanent employees, as well as visitors, about data collection and the use of video surveillance systems
- Collect only the data that is strictly necessary for the management of operations and avoid excessive collection of information about employees

Biometric data

In March 2024, the AEPD issued an urgent precautionary measure under Article 66.1 of the GDPR against Tools for Humanity, the operator of the Worldcoin project. The measure ordered the immediate suspension of biometric data collection and processing in Spain. The decision was based on several suspected GDPR infringements, including (i) insufficient information provided to data subjects, (ii) processing of minors' data without proper age verification, and (iii) the absence of mechanisms for withdrawing consent or exercising the right to erasure.

In parallel, the CNPD adopted a 90-day suspension of Worldcoin's activities in Portugal. The decision was based on multiple complaints regarding the collection of biometric data from minors, the failure to provide clear and accessible information to users, and insufficient safeguards for obtaining consent and ensuring data deletion. The CNPD stressed the urgency of this measure due to the risk of serious violations of data subjects' rights.

These actions culminated on December 19, 2024, when the Bavarian Data Protection Authority ("BayLDA"), acting as the lead supervisory authority under Article 60 of the GDPR, issued a binding resolution on the matter. In its resolution, the BayLDA found that Worldcoin had infringed several key GDPR provisions, including Articles 6.1 and 9. It concluded that biometric data had been processed without a valid legal basis and lacked the required security measures for special data categories. The BayLDA also confirmed the AEPD's precautionary measure and ordered the permanent deletion of all iris codes collected since the beginning of the project. It further required that any future processing rely on **explicit consent**, include the **right to erasure**, and **incorporate safeguards to prevent the processing of minors' data**. The resolution included the possibility of imposing administrative fines for non-compliance, and a separate enforcement procedure will follow under German administrative law.

Privacy and data protection | Supervisory authority decisions

General data protection principles

The Dutch Supervisory Authority ("PA") launched an investigation into Uber following more than 170 complaints about **information given to the data subjects and transfers of personal data outside the European Economic Area ("EEA")**.

During this investigation, it was ascertained that Uber had collected and stored sensitive information about European drivers on servers in the US without adopting the appropriate transfer methods. This information included account data, cab licenses, location, photographs, payment details, identity documents, and, in some cases, criminal and medical data.

Consequently, the AP imposed **a fine of €290 million,** which is its third fine since 2018 for **personal data breaches and failure to comply with information duties**.

ACTION POINTS

- Ensure that all transfers of personal data outside the EEA are performed using appropriate transfer mechanisms, in accordance with the GDPR
- Provide clear and complete information to data subjects on how their personal data is collected, used, stored, and transferred, complying with all the information obligations established by the GDPR

Privacy and data protection | EU legal content

EU–US privacy Framework FAQ

The EDPB published FAQs on the **EU–US data privacy framework**, aimed at facilitating the transfer of personal data between the two regions while ensuring an adequate level of data protection.

This privacy framework was developed in response to concerns raised by the CJEU, which led to the invalidation of the previous EU–US Privacy Shield.

The EDPB guidelines highlight the need for **transparency**, adequate **security** measures, respect for **data subjects' rights**, and effective **appeal and supervision** mechanisms.

Additionally, the EDPB provided **recommendations for companies**, such as conducting DPIAs and creating clear privacy policies, aimed at promoting a safe and efficient transfer of data, protecting data subjects' fundamental rights.

ACTION POINTS

- Implement international data transfer procedures that are clear and comply with EU international transfer requirements
- Enter into data processing agreements on the processing of personal data with third parties to ensure data transfers comply with GDPR requirements

Privacy and data protection | EU legal content

Data regulation FAQ

The European Commission published FAQs on the Data Act, a legislative proposal that aims to regulate access to and use of data in the EU, promoting innovation and competitiveness.

The Data Act establishes a legal framework for the sharing of data between companies, consumers and public authorities, ensuring the protection of data subjects' rights and data security.

The FAQs highlight:

- who can access the data and under what conditions;
- the obligations of the parties involved;
- the interoperability of data systems; and
- responsibility for data management and the necessary security measures.

It also proposes mechanisms to resolve disputes related to data access and use, such as mediation and arbitration, aimed at creating a single data market in the EU.

See our Legal Update: *Data Act: finally approved by the European Parliament*

Privacy and data protection | 2025 forecast

01

Applicability of the Data Act

The Data Act will become applicable in 2025. It aims to ensure that data generated by connected devices and digital services can be accessed and used by different parties, promoting innovation and competitiveness in the European market.

02

Regulation on the European Health Data Area

Discussions are expected to progress on the proposal for a regulation on the European Health Data Space, the purpose of which is to create a common European area where individuals can control their electronic health data (COM 2022/197).

03

Procedural rules relating to the GDPR

Progress is expected on the proposal for a regulation aimed at establishing procedural rules for handling complaints and conducting investigations under the GDPR (COM/2023/348).

04

Standard contractual clauses for data transfer

The European Commission is expected to publish standard contractual clauses for situations in which a data importer subject to the GDPR is located in a third country.

Telecommunications and technology

Spain:

Spain's regulatory and policy landscape in telecommunications and digital infrastructure underwent significant changes in 2024, highlighted by the following key developments:

- Royal Decree 443/2024: Establishes the **National Security Framework for 5G**, establishing cybersecurity obligations and enabling the classification of high-risk suppliers.
- Draft Bill on the Protection of Minors in Digital Environments: Proposes enhanced online protections for children, including **raising the minimum age for social media access from 14 to 16.** It also introduces mandatory parental controls on digital devices and digital restraining orders to prevent harmful online contact.
- Royal Decree 676/2024: Transforms the State Agency of Microelectronics and Semiconductors into the **Spanish Agency for Technological Transformation (SETT)**, centralizing strategic investments in semiconductors, microelectronics and critical digital infrastructure.

These legislative measures align with and expand upon the long-term goals set out in the España Digital 2025 agenda, fully integrated into the **National Recovery, Transformation and Resilience Plan** adopted by the Council of Ministers in April 2021 and subsequently approved by the European Commission.

Telecommunications and technology

Portugal:

The year 2024 was marked by technological innovation. In this section, we highlight the **National Digital Strategy,** which targets people, companies, state, and infrastructure. It aims to position Portugal as a leader in digital transition by 2030.

In the telecommunications area, we highlight the 2024 decision of the Portuguese Constitutional Court, declaring the unconstitutionality with general mandatory force of the rules contained in Ordinance 1473-B/2008, approved by ANACOM, charging **fees to providers of Tier 2 electronic communications networks and services**. In particular, the court decided that these rules breached the principle of the rule of law, which must be enacted by Parliament.

Telecommunications and technology | EU legislation

Regulation on the freedom of the media

Regulation (EU) 2024/1083 of the European Parliament and of the Council of April 11, 2024, establishes a **common framework for media services in the EU internal market**, aimed at protecting media freedom and pluralism (European Media Freedom Act).

This act harmonizes national rules to ensure a level playing field for media service providers, including the **audiovisual**, **radio** and **press sectors**.

Digitization and internationalization of the media have increased the importance of a coordinated approach to tackling challenges such as disinformation, manipulation of information and interference from third countries.

May 1, 2024	November 8, 2024	February 8, 2025	May 8, 2025	August 8, 2025	May 8, 2027
Entry into force	Application of the rule on the rights of media services recipients	Application of the rules on service providers' rights and duties, and the chapter on cooperation between authorities	Application of the section on regulatory cooperation and convergence	Application of the entire regulation, with the listed exceptions	Application of the rule on the right to personalize the media offer

ACTION POINTS

- Adopt measures to ensure that editorial decisions can be made freely within the company's editorial line
- Engage in structured dialogue with large-scale online platform providers to resolve content moderation issues and promote access to a diversified media offer
- Provide accurate and detailed information on the methodologies used to measure audiences, ensuring that they are transparent, impartial and verifiable, and submit them to annual independent audits to ensure their reliability and comparability

Telecommunications and technology | Spain legal content

SPAINS'S DIGITAL STRATEGY

Spain's national digital strategy is outlined in the **España Digital 2025 agenda**, launched in July 2020 and incorporated into the **Recovery, Transformation and Resilience Plan** approved in April 2021. This agenda aims to achieve a sustainable, inclusive and rights-based digital transformation by 2025. Its key objectives are as follows:

- Provide broadband connectivity of at least 100 Mbps to 100% of the population.
- Prepare the entire radio spectrum for 5G deployment.
- Equip 80% of the population with basic digital skills, with at least 50% being women.
- Train 20,000 new specialists in cybersecurity, AI and data.
- Make 50% of public services accessible through mobile applications.
- Boost e-commerce to account for 25% of SMEs' business volume.
- Reduce CO_2 emissions by 10% through digitalization.
- Increase audiovisual production in Spain by 30%.
- Ensure 25% of companies adopt AI and big data technologies.
- Establish a national charter on digital rights.

These objectives are structured around 10 strategic axes and align with the EU's digital policies.

Media action plan

In 2021, Spain launched a strategic initiative under the España Digital 2025 agenda, supported by €1.6 billion in public investment through 2025. Known as the ***Plan España, Hub Audiovisual de Europa***, the initiative aims to position Spain as a leading center for audiovisual production in the digital era, with a focus on achieving the following key goals:

- Increase audiovisual production in Spain by 30% by 2025.
- Attract international investment and talent to the Spanish audiovisual sector.
- Enhance the competitiveness of Spanish companies through new technologies.
- Promote gender equality and diversity in the audiovisual industry.

To meet these objectives, the plan implements measures across four main axes:

I. **Digitalization, internationalization and investment attraction**: This includes programs to internationalize the audiovisual sector, attract foreign productions, and create the "Spain Audiovisual Hub Bureau," a centralized information and support office

II. **Talent development and human capital**: This focuses on aligning training programs with industry demands, supporting company-led training initiatives, and promoting women's access to audiovisual education and qualifications.

III. **Improved financial and fiscal instruments**: The plan aims to facilitate access to financing and apply tax incentives for audiovisual production in Spain.

IV. **Regulatory reforms and administrative simplification**: Actions include simplifying administrative procedures and creating a digital one-stop shop for visas and work permits related to audiovisual projects.

Telecommunications and technology | Portugal legal content

PORTUGAL'S NATIONAL DIGITAL STRATEGY

Portugal's National Digital Strategy aims to position the country as a leader in **digital transition by 2030**, promoting:

- **digital inclusion;**
- **sustainability;** and
- **economic competitiveness**.

Structured around four main aspects (**people**, **business**, **state**, and **infrastructure**), the strategy includes objectives such as:

- increasing digital literacy;
- ensuring the safe use of technology;
- promoting gender equality in STEM fields;
- modernizing and digitizing administrative processes;
- expanding high-speed internet coverage; and
- strengthening cybersecurity and developing a sovereign cloud infrastructure.

Creating a national digital agency and implementing a national AI agenda are key actions to ensure robust digital governance and the ethical and safe adoption of new technologies.

Media action plan

The media sector faces significant challenges affecting the sustainability of companies and the stability of employees, putting pluralism and freedom of expression at risk.

The government undertakes to develop a comprehensive **plan** to tackle structural and cyclical problems arising from technological changes and consumer habits, ensuring the sustainability and independence of the media in Portugal.

Council of Ministers Resolution 105/2024 created the #PortugalMediaLab mission structure to coordinate and monitor the implementation of public policies, promoting transparency, pluralism, diversity, and inclusion in the media, and bolstering public trust in the policy formulation and implementation process.

Telecommunications and Technology | 2025 forecast

01

Spain: España Digital 2025 agenda

In 2024, Spain reached a historic milestone in public spending on **research, development, innovation, and digitalization**, **allocating €13.6 billion**, an increase of nearly **€2.5 billion** compared to 2023.

This amount represents **68.3% of the total €19.9 billion budget**, marking one of the highest allocation rates in recent years. The funds were directed toward the digital transformation of SMEs, 5G, cybersecurity, sustainable tech innovation, and advanced digital skills training.

This investment is part of Spain's broader strategy under the **Recovery Plan** and **España Digital 2025 agenda**, reinforcing the country's technological and industrial sovereignty.

02

Portugal: National Digital Strategy 2030

Portugal's national digital strategy will position the country as a leader in the digital transition by 2030, promoting digital inclusion, sustainability, and competitiveness.

It is expected that there will be developments regarding the changes and improvements listed, primarily regarding bolstering the digital skills of the population and resources to respond to cybersecurity incidents occurring in the public administration.

Cybersecurity

Three supplementary delegated regulations to the DORA Regulation were approved, introducing various technical standards related to classifying incidents and managing risks associated with information and communication technologies ("ICT"). Additionally, the European Commission approved the Cyber Resilience Regulation, aimed at establishing harmonized cybersecurity standards for digital products in the EU. At the same time, various rules have been established for applying the NIS2 Directive.

Cybersecurity | EU legislation

Delegated Regulation (EU) 2024/1772

Commission Delegated Regulation (EU) 2024/1772 of March 13, 2024, supplements Regulation (EU) 2022/2554 (DORA Regulation) by establishing technical standards for the classification of ICT-related incidents and cyber threats in the financial sector. It aims to harmonize and simplify incident reporting requirements for different types of financial entities.

Entry into force: April 2, 2024 ▶ Application of the regulations

Delegated Regulation (EU) 2024/1773

Commission Delegated Regulation (EU) 2024/1773 of March 13, 2024, supplements Regulation (EU) 2022/2554 (DORA Regulation) by establishing technical standards for the use of ICT services provided by third parties in critical financial sector roles.

ACTION POINTS

- Review and update the current policies and procedures for detecting and responding to cyber threats and information security incidents
- Review the entity's current risk matrix and update it according to the threat landscape in line with the sector of activity, size, and exposure to risk
- Update the procedures for classifying and reporting security incidents

- Develop clear procedures for analysis prior to hiring third-party ICT services, or review and update existing procedures
- Develop security, technical and human capacity analysis forms for the provision of ICT services, focusing on the risk associated with the service and the ability to maintain and continue operations in the event of a security incident
- Include the purchasing, legal, IT, DPO, and compliance departments in the prior analysis of the provider, as well as its human resources, when initiating the provision of services to the entity covered by the DORA Act
- Develop/update a register of the entity's ICT providers and their importance for maintaining the business activities

Cybersecurity | EU legislation

Delegated Regulation (EU) 2024/1774

Commission Delegated Regulation (EU) 2024/1774 of March 13, 2024, supplements Regulation (EU) 2022/2554 and establishes technical standards for managing the risk associated with ICT technologies in the financial sector to ensure the digital operational resilience of financial entities.

Entry into force: April 2, 2024 ▶ Application of the regulation

ACTION POINTS

- Review the financial entity's risk-related principles, policies and procedures in line with the current threat landscape, current and emerging vulnerabilities, and the entity's level of exposure to potential cyber attacks
- Review the risk classification of the entity's ICT services, products, or assets, and identify the interdependencies between them for the provision of the service

Cybersecurity | EU legislation

Rules for applying the NIS2 Directive

The Commission's Implementing Regulation of October 17, 2024, establishes rules for the application of Directive (EU) 2022/2555 ("NIS2 Directive") as regards the technical and methodological requirements of cybersecurity risk management measures established in Article 21.2 of the NIS2 Directive and further specification of the cases in which a cybersecurity incident is considered to be significant under Article 23.3 of the NIS2 Directive, with regard to DNS service providers, TLD name registries, cloud computing providers, data center service providers, content and distribution network providers, managed service providers, managed security service providers, online marketplace providers, online search engines, social networking services platforms, and trust service providers.

Entry into force: November 2, 2024 ▶ Application of the regulation

ACTION POINTS

- Review and update, based on this regulation, the entity's security plan, focusing on effective measures for identifying, preventing and mitigating information security risks
- Implement/review the incident response procedure, particularly by analyzing and defining the criteria for classifying a cybersecurity incident as "significant," based on the specifications of Article 23.3 of the NIS2 Directive
- Implement continuous monitoring systems to assess the effectiveness of the applied cybersecurity measures, with a regular audit and update plan

Cybersecurity | EU legislation

Cyber Resilience Regulation

Regulation (EU) 2024/2847 establishes horizontal cybersecurity standards for digital products in the EU, applying to all hardware and software products with digital elements.

This regulation requires manufacturers, importers and distributors to adopt safety measures from the product design phase, promoting stringent assessments to identify and mitigate risks, keeping detailed records, and ensuring CE marking.

Manufacturers must also report vulnerabilities and cybersecurity incidents to the pertinent authorities, such as the European Union Agency for Cybersecurity ("ENISA") and the CSIRT network, within specific deadlines, and provide continuous security updates.

See our Legal Update: *Cyber Resilience Act*

August 2, 2024	February 2, 2025	August 2, 2025	August 2, 2026
Entry into force	Application of notification and compliance provisions	Application of manufacturers' information obligations	Full application of the regulation

ACTION POINTS

- Review the information security management systems and update them in line with current reference standards for product security
- For manufacturers: Ensure compliance with technical security and risk management measures for digital products
- For importers and distributors: Develop or adapt a product analysis process in line with the standards and safety measures required by the regulation
- Establish protocols and processes for reporting and sharing information on threats, risks and vulnerabilities associated with digital products
- Review/develop policies and procedures to continuously update and monitor digital products and ensure the ability to detect, respond to, and eliminate risks when they arise in products
- Establish incident response procedures for the competent supervisory authority, with defined notification criteria, classification, and content

Cybersecurity | EU legislation

Cyber Resilience Regulation | Non-compliance

Failure to comply with the **basic cybersecurity requirements** established in Annex I and Articles 13 and 14:

- Fines of up to €15 million or, if it is a company, up to 2.5% of its total annual worldwide turnover in the previous financial year

Failure to comply with obligations imposed on **manufacturers**, **importers** and **distributors**, provisions relating to the declaration of conformity and affixing CE marking, technical documentation, conformity checks, and access to data and documentation:

- Fines of up to €10 million or, if it is a company, up to 2% of its total annual worldwide turnover in the previous financial year

Providing **incorrect or misleading information** to the notified bodies and market surveillance authorities:

- Fines of up to €5 million or, if a company, up to 1% of its total worldwide turnover in the previous financial year

Cybersecurity | EU–US joint statement

EU–US Joint Statement on CyberSafe Products Action Plan

The EU–US Action Plan on Cybersecurity and **IoT** for consumers aims to strengthen transatlantic cooperation on cybersecurity, especially in the context of the Internet-of-Things (IoT) and consumer products.

This plan recognizes the growing interconnectedness of IoT devices and the need to ensure that these devices are secure and resilient against cyber attacks. Collaboration between the EU and the US is seen as key to establishing common standards and practices that can be adopted worldwide, promoting a safer digital environment for consumers and businesses.

ACTION POINTS

- Develop and implement specific security standards for IoT devices in collaboration with manufacturers and regulators, including requirements such as authentication, encryption, and automatic updates, ensuring the security of devices throughout their lifecycle
- Develop practical guides for manufacturers, suppliers and consumers
- Establish transatlantic cooperation mechanisms to share real-time information on threats, vulnerabilities and cyber attacks, enabling a rapid and coordinated response to security incidents
- Invest in research and development between the EU and the US to promote advanced cybersecurity technologies applicable to IoT devices and digital infrastructure, strengthening technological competitiveness

Cybersecurity | 2025 forecast

01

Digital operational resilience of the financial sector (DORA)

Target entities must be in full compliance with this regulation from January 17, 2025.

Among other measures, companies should have rigorous systems and processes in place to identify, protect, detect, respond to, and recover from cybersecurity incidents, and to ensure the continuity of critical services even in situations of significant disruption, while maintaining transparent communication with customers and stakeholders about their operational resilience.

The DORA Regulation is expected to promote a more secure and resilient financial environment, reducing the risks associated with technological failures and cyber attacks, both for financial entities and their ICT providers.

02

Regulation on cyber solidarity

Collaboration is expected to be promoted between companies and national authorities by sharing information and resources to improve incident response. Creating a pan-European infrastructure of security operations centers (SOCs) and implementing a cybersecurity emergency mechanism will be important to guarantee a coordinated and effective response to threats, ensuring the continuity of critical services and the protection of sensitive data.

03

Transposition of the NIS2 Directive

On May 7, 2025, the European Commission issued a reasoned opinion to 19 Member States—including Portugal and Spain—for failing to fully transpose the NIS2 Directive.

The transposition of the NIS2 Directive will require target entities to implement stringent network and information security measures, including effective risk management adapted to the sector of activity and level of exposure.

Throughout 2025, the Portuguese National Cybersecurity Center (CNCS) will provide tools to support risk analysis and other mandatory security measures. The national cybersecurity reference framework is also expected to be updated, enabling greater support in implementing the security measures required by NIS2. Collaboration with national authorities and transparent reporting on security incidents will be crucial for compliance with NIS2.

Cybersecurity | 2025 forecast

04

EU Cybersecurity Act revision

The initiative to revise the Cybersecurity Act aims to clarify ENISA's mandate and enhance the European Cybersecurity Certification Framework, improving overall resilience.

It seeks to streamline, simplify and expand EU legislation to create a more user- and business-friendly cybersecurity framework while supporting a secure and resilient supply chain.

The Commission is holding a public consultation on the initiative from April 1, 2025, to June 20, 2025. During this period, it will collect feedback that it will use to help develop and refine the initiative.

05

EU Cybersecurity Blueprint recommendation

The European Commission has proposed a new cybersecurity blueprint to strengthen **coordination during cyber crises**. It defines the roles of EU actors and promotes collaboration between civilian and military entities (including NATO) to enhance cyber resilience.

The blueprint updates the EU framework for Cybersecurity Crisis Management, emphasizing preparedness, shared situational awareness, detection capabilities, and response and recovery tools to deter, mitigate and contain cyber incidents.

Advertising and consumer law

The year 2024 will be remembered as a significant milestone in the field of advertising and consumer law, especially regarding its development and regulation in light of the **digital single market**. In a context of technological advances and changing consumer habits, the EU has taken the lead in creating a **legal and ethical framework for the responsible use of** these practices, underscoring its commitment to safe and sustainable innovation, as well as responsible advertising.

With the implementation of the **new Product Liability Directive**, together with the **Digital Services Act**, the EU is consolidating its position as a global leader in the regulation of consumer practices, keeping up with innovation at the various stages of its development. We are also moving toward an environmentally conscious legislative framework, in line with the environmental strategy adopted by the EU in recent years, with the **review of the repairs regime** and the creation of **new duties of information and prevention of unfair commercial practices** aimed at bringing more transparency to advertising claims, making it easier for consumers to make informed purchasing decisions.

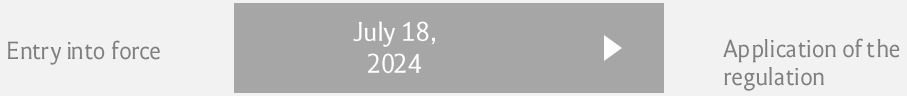
As we move into 2025, the forecasts indicate a year of regulatory transition and increasing adoption of **innovative business practices** in strategic sectors. It is essential that transposition into Portuguese law is thorough and balanced, with clear and objective rules that enable these standards to be applied effectively. The new legislation must seek to **balance product safety**, **sustainability** and **companies' ability to adapt**, considering consumer rights and technological progress, to create a fair and dynamic market.

Consumer law | EU legislation

Regulations for the design of sustainable products

The Ecodesign Regulation for Sustainable Products integrates essential measures to achieve the goals set by the 2020 Circular Economy Action Plan. In general, the regulation aims to substantially increase the circularity, energy efficiency and various other aspects concerning the environmental sustainability of products sold on the European market.

See our Legal Flash: *EU publishes ecodesign regulation*



Ecological Transition of Products Directive

This directive amends some of the main consumer law directives, creating new unfair commercial practices and new information requirements aimed at increasing transparency in consumer communications. The measures included in this directive impose restrictions on the advertising of products and services, labeling, and liability claims when the consumer decides to incorporate parts or accessories from third parties.

See our post: *Amendments to consumer directives to prevent greenwashing*

ACTION POINTS

- Adopt design practices that increase the durability, repairability and recyclability of products
- Develop systems to trace the origin of the materials and components used and provide consumers with clear and accessible information on the sustainability of products
- Invest in technologies that reduce energy consumption during production and implement measures to reduce carbon emissions throughout products' lifecycle

- Change the terms and conditions to comply with the new information requirements
- Review advertising communications to avoid unfair commercial practices
- Review the claims made in product labeling

Consumer law | EU legislation

Directive Promoting the Repair of Goods

Directive (EU) 2024/1799 changes the repair obligations of manufacturers and sellers for defective goods sold to consumers.

See our post: *EU imposes new repair obligations on manufacturers and sellers*

Entry into force: July 30, 2024 ▶ July 31, 2026 Deadline for transposition

Product Liability Directive - Adapting to technological advances

Directive (EU) 2024/2853 of the European Parliament and of the Council of October 23, 2024, replaces Directive 85/374/EEC, updating the liability regime for defective products to include technological advances such as AI, new circular economy business models and global supply chains. The directive broadens the concept of "product" to include software and digital products, strengthens the liability of manufacturers and economic operators such as importers and distributors, and establishes a strict liability regime. It also emphasizes transparency and traceability in the supply chain, requiring detailed records to facilitate the identification and recall of defective products, promoting more responsible and safer business practices.

See our Post: *New directive on liability for defective products*

Entry into force: December 8, 2024 ▶ December 9, 2026 Deadline for transposition

ACTION POINTS

- Change the terms and conditions to ensure compliance with the new rules
- Review the procedures for responding to complaints/exercising consumer rights
- Prepare the EU information form on repairs

- Implement continuous software monitoring and updating procedures to identify and correct vulnerabilities in company products
- Document and keep detailed records documenting product compliance with EU and national safety requirements
- Develop incident response plans detailing the procedures to be followed in the event of security breaches or product defects

Consumer law | EU legislation

General Product Safety Regulation

Regulation (EU) 2023/988 of the European Parliament and of the Council on general product safety establishes essential rules on the safety of consumer products made available on the market and aims to respond to recent technological advances, the growing globalization of markets and supply chains, and the increase in distance and online sales.

ACTION POINTS

- Ensure that the products made available comply with the general safety requirement
- Use the Safety Gate and Safety Business Gateway platforms to provide information related to product safety
- Comply with consumer-information obligations and ensure compliance by contracted economic operators

Consumer law | 2025 forecast

01

Transposition of the Consumer Empowerment Directive for the Ecological Transition of Products

The transposition of the Consumer Empowerment Directive for the Ecological Transition of Products into national law will bring significant changes to commercial practices and consumer protection. The transposition into both Portuguese law and Spanish law is expected in 2025.

Companies will have to adjust their **marketing and advertising strategies** to avoid misleading claims about the environmental and social characteristics of products, and unsubstantiated claims will be prohibited.

Companies will have to provide evidence for any environmental claim and clear information on the **durability**, **repairability** and **upgrades** of the products they place on the market, as well as greater transparency regarding warranties and after-sales services (including communication of environmentally friendly delivery options).

These changes will require internal adaptations and investments in certifications, as well as awareness-raising and training for the employees involved in these processes.

02

Transposition of the Directive Promoting the Repair of Goods

The transposition of the Directive Promoting the Repair of Goods into national law will bring significant changes to the repair obligations of manufacturers and sellers. The transposition into both Portuguese law and Spanish law is expected in 2025.

The directive imposes on sellers **the duty to inform** consumers of their right to choose between **repair and replacement** and to extend the warranty period by a further 12 months if the consumer chooses repair.

Manufacturers must repair certain goods and publish indicative repair prices on their websites, in addition to providing spare parts and tools at affordable prices.

The legal concept of the repairer is created to facilitate access to qualified and efficient repair services to promote sustainability and circular responsibility for products placed on the market.

Conclusions

Artificial intelligence

The entry into force of the AI Act and the creation of the European Artificial Intelligence Office have strengthened Europe's position as a global leader in regulating AI systems.

Companies must be aware of the new obligations and the substantial penalties for non-compliance, besides ensuring compliance with EDPS and OECD recommendations.

Intellectual property

The modernization of the industrial design protection system and measures to combat counterfeiting stand out as important advances.

Companies must adapt to the new registration rules and adopt advanced technologies to protect their IP rights.

Privacy and data protection

The consolidation of the concepts and methods of collecting and processing personal data, along with the EDPB guidelines and court judgments, underscore the growing importance of compliance with the GDPR.

Companies must ensure transparency and security in processing personal data, especially in international transfers.

Telecommunications and technology

Spain and Portugal are making significant progress with ambitious national digital strategies and investments.

Companies must be prepared for regulatory changes and make the most of technological innovation opportunities.

Cybersecurity

The DORA Act and the Cyber Resilience Act establish harmonized cybersecurity rules for digital products.

Companies must review and update their security policies and incident response procedures to ensure operational resilience.

Advertising and consumer law

The Product Liability Directive and the Digital Services Act reinforce the EU's position in regulating consumer practices.

Companies must adopt transparent and sustainable commercial practices, ensuring product safety and consumer protection.

The forecasts for 2025 point to a regulatory transition and increasing adoption of innovative practices in strategic sectors.

It is essential that companies adapt to the new legal and technological requirements, ensuring compliance and competitiveness in the European market.

What we offer

We advise on all areas of business law and help our clientes with the most demanding matters, in any territory, providing the experience and knowledge of specialized teams.

29 Legal specializations	**+2000** Professionals
25 Offices in 12 countries	**29** Nationalities & 16 languages
+300 Lecturers & 8 professors	**26%** Women in top positions

FT INNOVATIVE LAWYERS EUROPE 2024 WINNER

Europe's most innovative firm in "Talent management", 2024

Most innovative firm in continental Europe, 2023

IFLR AWARDS 2025 EUROPE WINNER

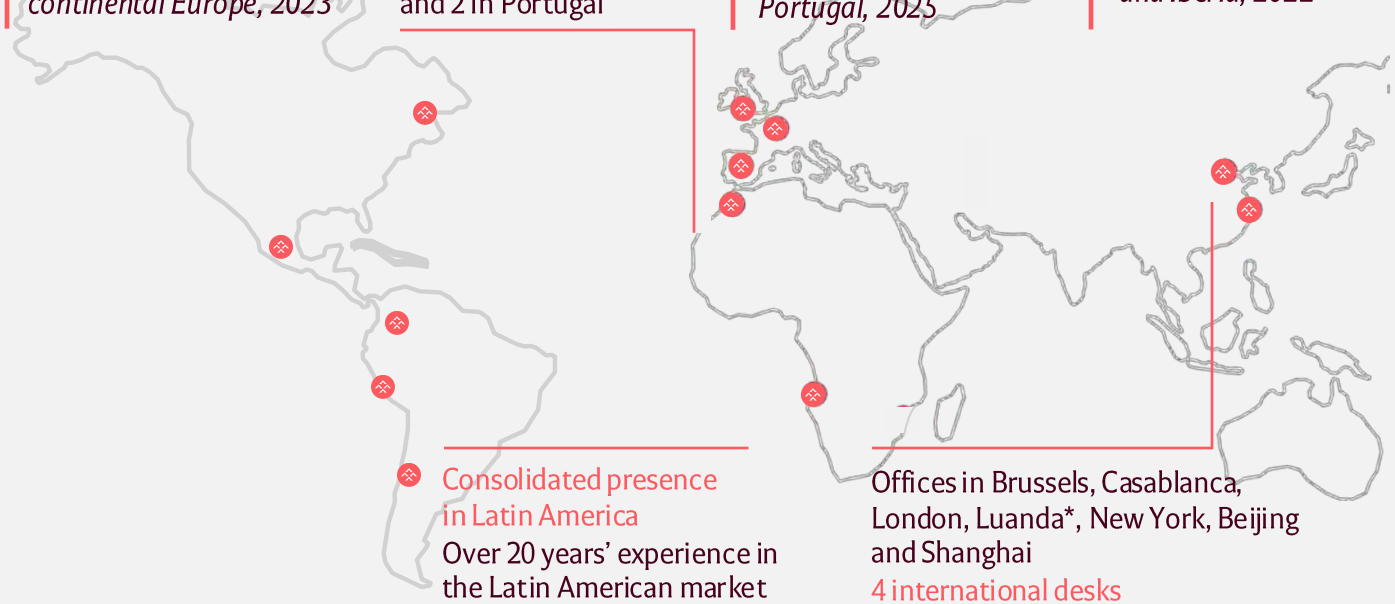
EU Firm of the Year, 2025

National firm of the Year: Portugal, 2025

THE LAWYER

Highly commended in Iberia, 2024

Firm of the year in Europe and Iberia, 2022



Maximum presence in the Iberian Peninsula
13 offices in Spain and 2 in Portugal

Consolidated presence in Latin America
Over 20 years' experience in the Latin American market and offices in Chile, Colombia, Mexico and Peru

Offices in Brussels, Casablanca, London, Luanda*, New York, Beijing and Shanghai
4 international desks
European network with leading firms in Germany, France and Italy

*In collaboration with local law firms.

Experts in all practice areas of business law

- Business-oriented knowledge with a sectorial approach.
- Maximal specialization combined with the latest technology.
- Knowledge and innovation team, with over 40 academics and specialists for innovative solutions.

CUATRECASAS ESG

We comply with environmental, social, and good governance (ESG) criteria in providing our services and in our internal management.

Here we detail the main parameters by which we measure our ESG performance.

See also our latest Business Report.

GOLD 2023 ecovadis Sustainability Rating

Practical guides

Doing Business in Spain 2025 edition

Doing Business in Portugal 2025 edition

EU AI Act: Practical guide

Market trends in Iberian private equity transactions

Cuatrecasas Arbitration Highlights - Number 4

Restructuring in Iberia and LatAm

10 keys to venture capital transactions in Spain

10 keys to venture capital transactions in Portugal

Key contact persons

Joana Mota Agostinho
Partner | Data Protection | Digital Technologies and Media (TMT)

View CV
joana.agostinho@cuatrecasas.com

Sónia Queiroz Vaz
Partner | Intellectual and Industrial Property, and Trade Secrets | Data Protection

View CV
sonia.queiroz.vaz@cuatrecasas.com

Albert Agustinoy
Partner | Digital Technologies and Media (TMT)

View CV
albert.agustinoy@cuatrecasas.com

Álvaro Bourkaib
Partner | Intellectual and Industrial Property, and Trade Secrets

View CV
alvaro.bourkaib@cuatrecasas.com

The information provided in this presentation has been obtained from general sources. It is for guidance purposes only and should be interpreted in relation to the explanations given. This presentation does not constitute legal advice under any circumstances.

A informação contida nesta apresentação foi obtida de fontes gerais, é meramente expositiva, e tem de ser interpretada juntamente com as explicações que a acompanham. Esta apresentação não pretende, em nenhum caso, constituir uma assessoria jurídica.

La información contenida en esta presentación se ha obtenido de fuentes generales, es meramente expositiva, y se debe interpretar junto con las explicaciones que la acompañan. Esta presentación no pretende constituir en ningún caso un asesoramiento jurídico.

CUATRECASAS