Just in Time

AI: Regulation, Rise and Challenges

Apr 2025

iason ESSENTIAL SERVICES FOR FINANCIAL INSTITUTIONS

Executive Summary

- Starting from the first release of Chat GPT, the interest surrounding **AI applications** has spread across **various industries** thanks to the potential of these technologies to **enhance productivity**, **increase efficiency**, and **drive economic growth**
- While the **AI** market and applications have shown **rapid growth** that is expected to **continue** in the **next years**, concerns about its implications for i.e., human rights, financial stability, and data protection have grown in parallel
- The advancement of **AI** and its **widespread** adoption **across various industries** has highlighted the **importance** of **coordination** in **regulatory oversight** among **international regulators**, as well as the need for **regulatory frameworks** that **embrace** a more **integrated approach** among **national authorities**
- In recent years, **supranational bodies** such as the OECD and UNESCO have **developed** several **guidelines** to assist regulators in addressing **AI-related challenges**, while **political**, **regional**, and **national frameworks** have been (or are currently being) developed to **prevent regulatory gaps** and **inconsistencies**
- Despite this, the **intrinsic nature** of **AI** requires these **efforts** to be more **widespread** in order to avoid **fragmentation** and **ensure consistent oversight**

At a Glance

Keywords: AI, Gen AI, AI Supervision, AI Act

01

The Rise of AI

A Brief Market View

Financial Markets Adoption

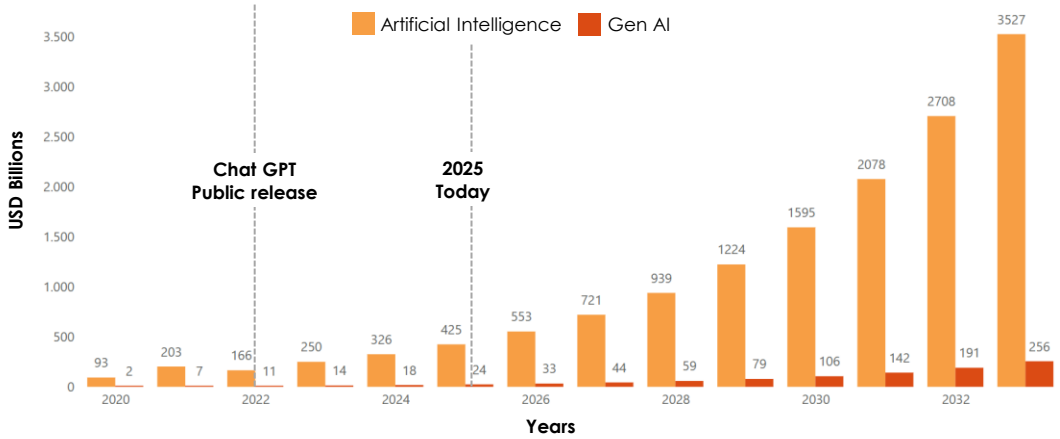
Across Non-Financial Industries Adoption

The Rise of AI 1/3

A Brief Market View

Since the **first release** of **ChatGPT** in 2022, **Artificial Intelligence** has gathered increasing **attention** from both **markets** and **regulators** due to its capability of profoundly **transforming** our **world** and **affecting productivity** and **economic growth**. As **industries** are **integrating AI applications** in a wide set of **processes**, **regulators** are **increasingly** focused on supporting this innovation with **robust regulatory frameworks**. The rise **AI applications** across **various industries** demands **collaboration** among **international authorities** to address **cross-sector challenges** and **avoid regulatory fragmentation.**

AI and GenAI Market Size Growth*



+31%
Expected CAGR

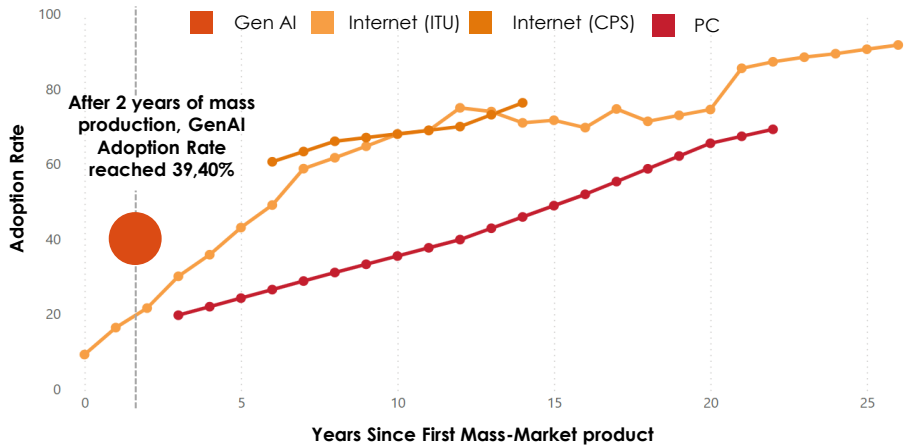
Since the **release** of **ChatGPT**, **AI** market growth has recorded a **+27% CAGR** with an **expected +31% CAGR** in the **next eight years**

+34%
Expected CAGR

Since the **release** of **ChatGPT**, **Gen AI** market growth has recorded a **+22% CAGR** with an **expected +34% CAGR** in the **next eight years**

*Data Market.US

Technologies Adoption Rate*



The data shows that, **compared** to other disruptive **technologies** that have had a significant impact on both markets and private lives, **GenAI** has reached an **adoption** rate of nearly **40%** in **just 2 years** after its mass introduction. For instance, PCs required nearly **10 years** to reach the same level of adoption, while the **Internet** took approximately **5 years**

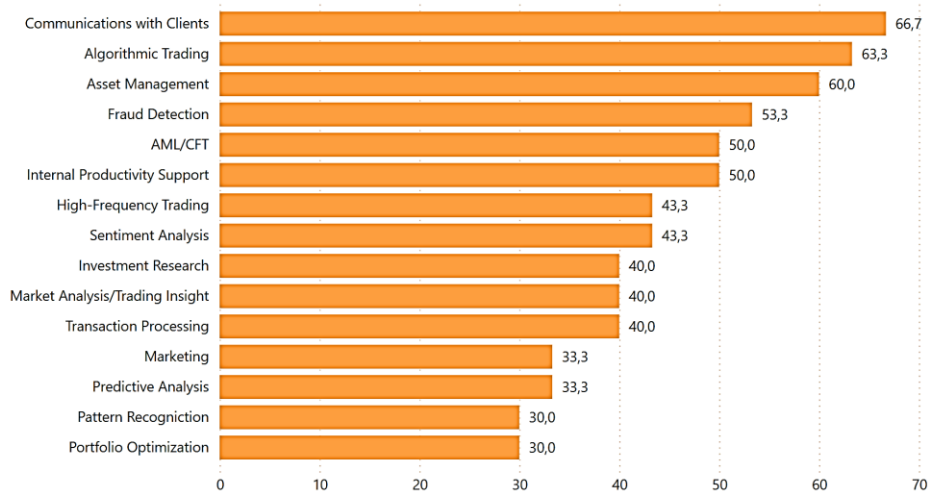
*Data: A.Bick, A.Blandin, D.Deming;The Rapid Adoption of Generative AI; 2024

The Rise of AI 2/3

Financial Markets Adoption

The **Financial Industry** has always been one of the **first adopters** of new **technologic innovations**, with the goal of **enhancing productivity** and **improving efficiency**. Regarding so, a survey carried out by FSA of Japan in March 2025 revealed that more than **90%** of the sample (over 130 international FIs) **broadly permits** the use of **AI** (70% also integrates GenAI). Always in March 2025, IOSCO published the results of a survey aimed to to **identify** the **current and the future potential usage of AI** in **financial markets, highlighting** the **wide spread** of **AI** in **FI processes.**

AI use cases*



The IOSCO's survey showed that AI is already used on a wide group of FI process with the most common use cases include **client communications**, **algorithmic trading** and **asset management**, followed by surveillance applications and productivity enhancement

*Data IOSCO Artificial Intelligence in Capital Markets: Use Cases, Risks, and Challenges; March 2025

Type of AI used By Market Participants

The IOSCO's survey also asked to specify the **types of AI** used by market participants for various applications. Results underline that **Machine Learning**, **NLP** (Natural Language Processing) and **LLMs** are the most widespread AI applications within the most AI-involved functions

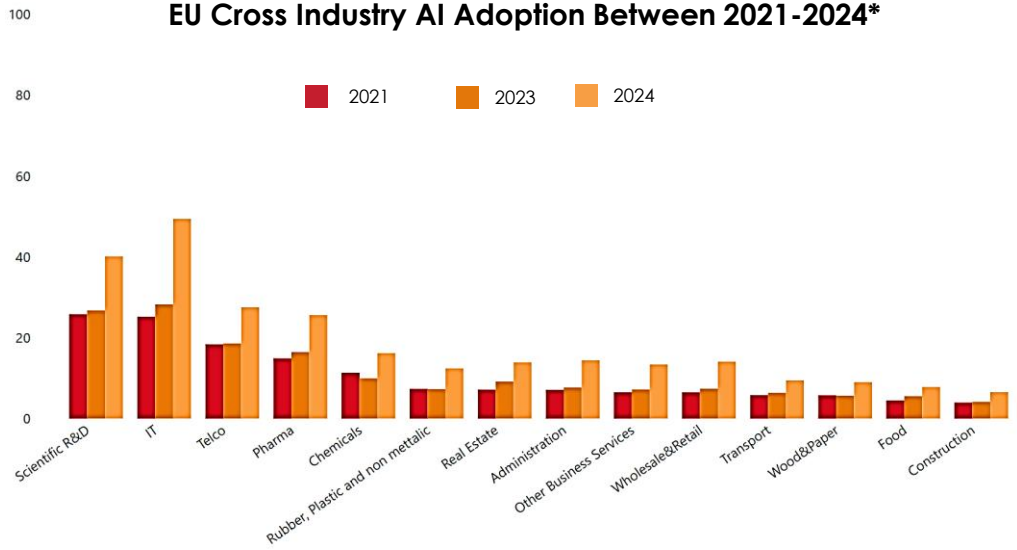
*Data IOSCO Artificial Intelligence in Capital Markets: Use Cases, Risks, and Challenges; March 2025

The Rise of AI 2/3

Financial Markets Adoption

The **adoption** of **artificial intelligence** (AI) **across markets** varies based on industry needs, regulatory frameworks, and the availability of data and infrastructure, progressing at different rates. While the financial and technology sectors are among the most advanced, other industries are still adopting AI applications at a slower pace.

EU Cross Industry AI Adoption Between 2021-2024*



Focusing on the EU, data shows an **overall growth trend** in **AI** adoption **across industries** between 2021 and 2024. In particular, markets characterized by traditionally technology-intensive applications, such as IT, R&D, telecom, and pharma, are experiencing an even steeper increase in adoption

*Data Eurostat

Examples of AI Adoption across industries

Telco

AI is being used to **optimize networks**, improve customer service, and **reduce** operational **costs**. Telecommunications regulators are studying the role of AI in network infrastructure management

Transport

AI is being used in transportation for **autonomous driving** systems by improving **road safety** and **reducing** operating **costs**, optimizing traffic by reducing traffic jams, and improving the efficiency of public transportation

Manufacturing Industry

AI adoption in manufacturing is **growing** at a **slow pace**, as integration with **existing processes** and high **upfront costs pose challenges**. However, its application in productivity enhancement, particularly through cobots and quality control, continues to expand

02

The Need for AI Oversight

Why AI Poses Unique Regulatory Challenges

Regulatory Challenges - Financial Stability

Regulatory Challenges - Data Protection

Regulatory Challenges - Intellectual Property

Regulatory Challenges - Competition

Regulatory Challenges - Telecommunication

The Need for AI Oversight 1/6

Why AI Poses Unique Regulatory Challenges

The **rapid advancement** of Artificial Intelligence has **intensified the need for robust oversight frameworks** capable of addressing its complex societal, ethical, and legal implications. **Unlike traditional technologies**, AI systems can evolve autonomously, operate opaquely, and influence critical decisions at scale, presenting **unprecedented regulatory challenges**. These include issues of accountability, transparency, bias, and cross-border governance, all of which demand **tailored** and **adaptive regulatory responses.**

Regulatory Risks

AI's **global reach**, reliance on **cloud infrastructure**, and **cross-sector impact** (finance, privacy, cybersecurity, competition) further **complicate regulation** requiring **policymakers** to face several **regulatory challenges** requiring specific expertise, tools, and huge resources, with the potential result of **insufficient oversight** and **growing systemic risks**. Other than that, the **lack** of **international coordination** could lead to **inconsistent standards** increasing the risk of **regulatory arbitrage**, while **AI-related menaces**, such as cyberattacks, can **spread rapidly**. To **mitigate** these **risks**, **regulators** must **enhance AI knowledge**, **update staff training**, and **adopt AI-powered tools** for more effective supervision

Finacial Stability

To ensure **financial stability** within the economic system **regulators** must **carefully watch** the **potential** effects of wide usage of **AI** within the market player in order to properly handle risks such as:

- **Third-party Risk Concentration Riks**
- **Market&Liquidity Risk**
- **Cyber Risk**

Data Protection

Effective **Data Governance frameworks** are integral to any **successful AI application**.
Market authorities' policy challenges, therefore, encompass both the models and the data they utilize, as for example:

- **Manipulation Risk**
- **Privacy Risk**
- **Compliance Risk**

IP

AI is reshaping the **intellectual property (IP)** landscape raising issues and risks which include:

- **Copyright issues with AI-generated works**
- **Uncertainty in patenting AI Technologies**
- **Lack of rules on AI Inventorship**
- **Ambiguity over data and content ownership**
- **Poor regulatory coordination**

Competition

AI markets pose **unique challenges** for **competition** authorities due to their rapidly **evolving structure** and reliance on **key inputs**. The main risks include:

- **Market concentration**
- **Ecosystem control**
- **Anti-competitive agreements**
- **Exclusionary acquisitions/ partnerships limiting market entry**

Telecommunication

Telecommunication faces a range of **AI-related risks** that reflect both **technical dependencies** and **governance challenges** such as:

- **Fragility of infrastructure essential to AI**
- **Unequal access to data**
- **Absence of common standards**
- **Gaps in cross-sector risk monitoring and regulatory coordination**

The Need for AI Oversight 2/6

Regulatory Challenges - Financial Stability

AI has been **widely integrated into financial intermediary processes** to **enhance efficiency** and **automation**. However, **financial markets** are **crucial** for **economic stability** and are deeply interconnected across borders. This necessitates strong collaboration between regulators and market players to assess and manage AI-driven risks effectively.

Third-Party Risk

The **financial sector's reliance on specialized hardware, cloud services** and **pre-trained models** creates substantial third-party dependencies. The market for these products and services is highly concentrated, exposing financial institutions to **operational vulnerabilities** if key service providers face disruptions

Market Stress And Liquidity Risk

The **widespread use** of common **AI models** and **datasets** can increase correlation in trading, credit, and pricing activities, **raising risks of market stress, liquidity crises,** and **asset price vulnerabilities**. It may also **concentrate resources**, **leading to an oligopoly** of a few major providers

Cyber Risks

The **growing use of AI increases the risk of cyberattacks**, as heavy data use, new interaction methods, and reliance on specialized providers expand potential vulnerabilities, raising both the frequency and impact of threats

Cross-Coordination with Regulatory Standards

The complexity and limited explainability of some AI models makes assessing their quality and reliability challenging. Ensuring **alignment** with **regulatory standards** becomes increasingly **difficult** as biases or low-quality data embedded in these models are **harder to detect and address**

The Need for AI Oversight 3/6

Regulatory Challenges - Data Protection

Effective Data Governance frameworks are **integral** to **any successful AI application**. Market authorities' policy challenges, therefore, encompass both the models and the data they utilize.

Privacy Risks and AI's Processing of Personal Data

AI technologies, including generative AI, rely heavily on the **processing of personal data**, which raises significant concerns regarding privacy, bias, and discrimination

Compliance with Global Data Protection Laws

Current data protection and privacy laws apply to the development and use of AI technologies, although **jurisdictions are increasingly adopting AI-specific laws** and **regulations** to address the unique challenges posed by these technologies

AI Surveillance and Manipulation Risks

One of the more complex challenges in the **intersection** of **AI** and **data protection** involves overseeing the processing of **personal data** in various AI applications, such as **facial recognition**, **manipulative AI tools targeting children**, **workplace monitoring**, and **Gen AI**

Need for Regulatory Coordination

As AI technologies continue to evolve, enhanced **cooperation of data protection authorities with** other **market supervisors** across different jurisdictions will be vital for establishing a trustworthy global AI ecosystem

The Need for AI Oversight 4/6

Regulatory Challenges - Intellectual Property

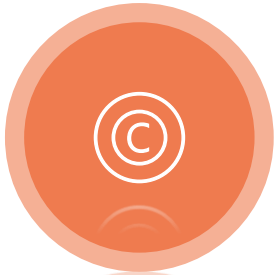
The rise of AI and machine learning presents complex challenges for **intellectual property** (IP) offices worldwide. As these **technologies blur traditional boundaries** of **inventorship, authorship,** and **ownership, existing IP frameworks are being tested**. IP authorities must grapple with issues such as the **patentability** of **AI-generated** inventions, **data ownership** in training sets, and the **legal status** of **AI-created works**. At the same time, **enforcement bodies face the task of balancing protection** with **innovation** and **public interest,** requiring **cross-sector collaboration** and **adaptive policy approaches.**

Patentability of AI Technologies

AI inventions often blur the line between **software and patentable subject matter**, raising doubts under existing patent frameworks like the EPC. Drafting compliant claims and applying traditional doctrines is particularly complex for AI-related inventions

Data Ownership and IP Rights

AI systems rely on large datasets, yet there is **legal uncertainty over who owns the IP in both the input and intermediate data**. This raises the need for potential new IP rights and alignment with data protection laws like the GDPR



Copyright and AI-Generated Content

Creative works generated by AI **challenge current copyright laws** on **authorship, originality, and ownership**. There are also concerns about potential infringement when AI reuses existing materials

Coordination and Policymaking

IP offices must **collaborate with data protection** and **competition** authorities to develop consistent, inclusive policies. **Ensuring alignment** with broader societal goals is key to responsible AI governance

Enforcement and Market Dynamics

Strong IP protections could reinforce the **dominance of big tech firms**, **restricting competition** and **access to information**. Enforcement bodies must balance rights protection with public interest and market fairness

Inventorship in AI-Created Innovations

If an AI system autonomously invents something, it's unclear who should be **legally recognized as the inventor**. This creates a gap in current patent systems, which assume human inventorship

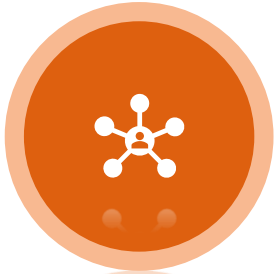
The Need for AI Oversight 5/6

Regulatory Challenges - Competition

As **AI-driven markets expand**, **competition authorities** are under **increasing pressure to monitor emerging dynamics** and **prevent anti-competitive practices**. Traditional concerns, such as **vertical integration** and **dominance** by **large tech firms**, are now amplified by the integration of **AI technologies**, requiring a more **proactive** and **nuanced regulatory approach.**

Complex Market Definition in AI

Defining relevant markets in AI is difficult due to its evolving nature. Authorities must distinguish between **upstream** (e.g. data, compute resources) and **downstream** (e.g. generative AI services) segments, using alternative metrics like usage or processing capacity



Network Effects and Ecosystem Control

Dominant firms can **restrict access** to essential AI components through **strategies** like **exclusivity** or **self-preferencing**. These behaviors can distort competition and reduce consumer choice

Risk of Anti-Competitive Agreements

Competition authorities must monitor **horizontal agreements** that may reduce competition or involve unlawful data sharing. Vertically integrated players may also use pricing strategies to disadvantage rivals

"Killer" Acquisitions

Large firms might **acquire emerging competitors** to eliminate future threats, which can hinder innovation and limit consumer options. These acquisitions **require close regulatory scrutiny**

Input Concentration Through Partnerships

Partnerships between **large firms and smaller developers**, while potentially beneficial, can lead to an **overconcentration** of key inputs such as data and computing power. This could **unbalance the market**, requiring ongoing oversight

The Need for AI Oversight 6/6

Regulatory Challenges - Telecommunication

The integration of AI depends on **robust**, **reliable** telecom **infrastructure**. As AI, IoT, and cloud systems converge, telecom authorities must ensure **resilient**, **low-latency**, and **interoperable networks** to support widespread and fair AI adoption

Infrastructure Dependance and Vulnerability

AI performance relies on **strong**, **stable**, **internet infrastructure**, and any **weakness** in **telecom networks** can **undermine AI Systems across sectors**. A strategic, coordinated approach is needed to address these infrastructure challenges

Unequal Access to Critical Enablers

AI deployment depends on access to reliable data, storage, processing power, and connectivity. **Uneven access to** these **resources' risks creating disparities** in **AI adoption** and **innovation**

Need for Standardisation

Lack of common standards can **slow AI adoption** and **increase costs**. Standardization helps promote interoperability, reduce development time, prevent vendor lock-in, and foster fair competition

Impact of AI on Telecom Network Design

AI's integration will reshape telecom networks, requiring new hardware, low-latency environments, and better alignment between software and physical infrastructure. This could lead to **decentralized data centers** and **increased network load**

Operational Transformation through AI

AI is expected to **automate telecom operations**, optimize networks, enhance customer service, and improve energy efficiency

Risk Monitoring and Cross-Sector Coordination

Telecom authorities must **develop tools to monitor AI-related risks** and collaborate with financial, competition, and data protection regulators. They should also explore AI use within their own institutions to **enhance policymaking** and internal operations

03

AI Regulation

A Timeline of Main Regulatory AI Milestones

Supernational Bodies' Approaches and Guidelines

National and Regional AI Regulatory Approaches

Europe – AI Act

AI ACT – Focus on Europe's National Approaches

AI ACT – Focus on Interconnections with NIST AI RMF

Canada – Digital Regulator Forums

UK – Digital Regulation Cooperation Forum

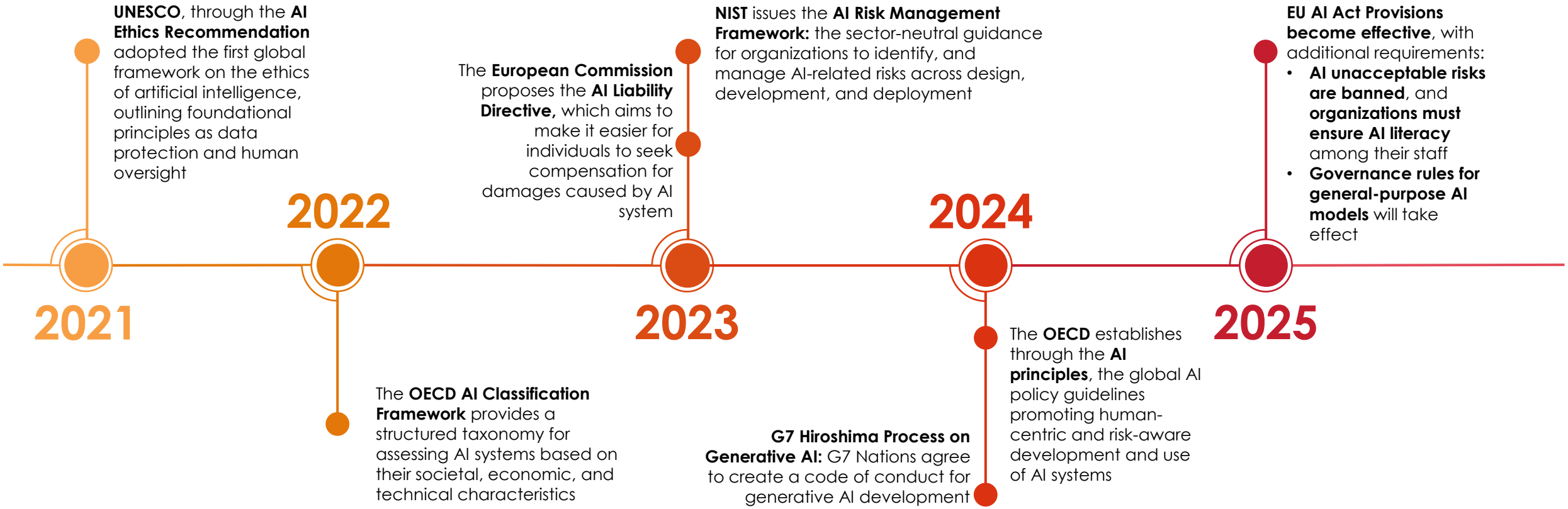
Australia – Digital Platform Regulators Forum

China Approach

AI Regulation 1/10

A Timeline of Main Regulatory AI Milestones

The path toward an **integrated** and globally **coordinated** regulatory **framework** for **Artificial Intelligence** is evolving through a series of key milestones. International summits, strategic proposals, and legislative initiatives, particularly within the European Union, reflect the **growing commitment to addressing AI-related risks**, **fostering** responsible **innovation**, and **harmonizing legal standards** across jurisdictions.



AI Regulation 2/10

Supernational Bodies Approaches and Guidelines

In response to the complex regulatory challenges posed by Artificial Intelligence, ranging from fragmented national policies to limited institutional expertise, **supranational bodies** have begun **implementing targeted frameworks** and **proposing guidelines** aiming to promote **transparency**, ensure **accountability**, and **harmonize oversight across borders.**

UNESCO
Ethic AI Recommendations

The recommendations were adopted and published in **November 2021** to promote the ethical use of AI. They outline **10 key principles** that must be encompassed in an **AI application life-cycle** (e.g. data protection, non-discrimination, sustainability, human oversight…).
The **recommendations** promote the **adoption** of **policies** that foster its principles including:

- **Ethical Governance**
- **Privacy and Data Protection**
- **Education and Sensibilization**
- **Minimizing impact on workers**
- **Internation cooperation**

OCED
Principles

A globally endorsed ethical **framework** guiding trustworthy **AI development**.
The **Principles** offer global **ethical guidelines** for trustworthy and **human-centric AI** aiming to support governments and foster **international collaborations** through tools, guides, and case studies via the **AI Observatory**. They also outline the importance of adopting policy to mitigate specific risks:

- **Harmful Bias**
- **Threats of Human Rights**
- **Lack of Transparency**

NIST
AI Risk Management Framework*

The NIST AI Risk Management Framework (AI RMF), published in January 2023, provides **guidelines** for organizations **designing**, **developing**, **deploying**, or **using AI systems**. Its goal is to help assess and **mitigate AI-specific risks**. The framework takes a sector-specific and technology-neutral approach, focusing on **4 core structures**:

- **Govern**
- **Map**
- **Measure**
- **Manage**

The framework identifies also specific applications of the **AI RMF Profiles**.
In January 2024, the NIST published the integration of AI RMF profile specific for GenAI Purpose

OCED
AI Classification Framework

Following the **OCED Principles**, it is established to **help regulators** in **assessing** and **classifying AI systems**.
The Framework identifies 5 key high-level dimensions to assess how AI systems operate and impact various facets of society, economy, and the environment:

- **People&Planet**
- **Economic Context**
- **Data&Input**
- **AI Model**
- **Task&Outputs**

The Framework offers a **comprehensive approach** to **analyzing AI systems** allowing users to identify AI-specific risks following a generic approach ensuring its application across different contexts

*To a complete overview of the framework: D.Esposito, B.Ghilardi; AI Risk Management Framework; JIT N.117; Feb 2023

AI Regulation 3/10

Some National and Regional AI Regulatory Approaches

At national and regional level, there are already few examples of regulators **addressing AI regulation** through a **broad approach**, including different market authorities in the dialogue, development and enforcement of AI regulatory framework.

Digital Regulators Forum (Canada)
Aims to foster **collaboration** and **information sharing** among regulators to facilitate consistent regulatory approaches

Digital Regulation Cooperation Framework (UK)
Involves **several UK's authorities** to address digital regulation challenges, including those posed by AI

AI ACT (European Union)
Aims to establish a **harmonized** set of **rules** for all the life-cycle phase of **AI** applications in the EU

AI Regulations & Governance (China)
Involves **multiple state authorities** to regulate AI with a centralized approach, ensuring **alignment** with national security and policies

Digital Platform Regulators Framework (Australia)
Involves several Australian authorities to address issues and challenges related to **digital platforms**

AI Regulation 4/10

Europe – AI Act

The **AI Act*** is the **first cross-jurisdictional regulatory framework** focusing on **Artificial Intelligence**, establishing a **harmonized** set of **rules** for the **development**, **market introduction**, **deployment**, and **use** of **AI** in the EU. The regulation **applies** across the entire **AI value chain** and defines a **risk-based approach** to set **requirements** and **obligations.**

Who

The **AI Act** applies to **several parties** in the **AI value chain**:

- **Providers**: Developing or placing AI systems on the market
- **Deployers**: Using AI systems for professional activities
- **Distributors**: Making AI systems available in the EU
- **Importers**: Placing AI systems from non-EU entities on the EU market

What

The **AI Act** applies to **all AI systems** that fall under the AI System definition outlined in the AI Act Art 3.

In **February 2025**, the **EC** published the official **guidelines** to assist in **determining** whether a system constitutes an **AI system and** to provide the criteria for a clear interpretation of **Prohibited AI practices**

How

AI Act applies **a risk-based approach** that ranks **AI systems** in the four following categories, based on their **risk** for **society's stability** and **people's safety**:

- **Unacceptable** Risk
- **High**-Risk
- **Limited**-Risk
- **Lower**-Risk

Enforcement

The **AI Enforcement** is designed to ensure a **complementary division** of **roles** between the **European Commission** and the **National Authorities**. The **European Commission oversees general-purpose models** with **power** to adopt **delegated acts**, meanwhile, the **National Authorities** of each Member State are **responsible** for **enforcing** the **risk-based rules** for AI systems

* For a deep dive into the AI Regulatory Framework see Artificial Intelligence Act (AI Act) and AI Act: AI System Definition and Prohibited AI Practices

AI Regulation 5/10

AI ACT – Focus on Europe's National Approaches

As the AI Act comes into effect, member states are **establishing national coordination frameworks** to align fragmented oversight, address risks, and ensure compliance. The following shows how Italy, France, and the Netherlands are planning to leverage centralized entities and inter-agency collaboration to **harmonize AI governance.**

Italy
2024-2026 Strategy for AI

- Italy's 2024 Draft Law tasks the **Cybersecurity Agency** and the **Agency for Digital Italy** (AgID) with **coordinating AI Act implementation**
- A **committee** of director-generals from key authorities, supported by the Presidency, ensures **alignment across institutions**
- The focus is **harmonizing oversight** to **prevent fragmented governance and** addressing overlaps between agencies
- Collaboration between authorities aims to manage AI risks, particularly compliance and cross-sector challenges
- **Centralized coordination promotes shared strategies**, reducing legal gaps and ensuring cohesive regulation

France
Network of Digital Regulators

- France's 2024 Law creates a **national network connecting regulators** (e.g. Competition Authority, Data Protection Authority) **and ministries**
- It uses two layers: a **high-level steering body for strategic planning** and a **technical group** for detailed policy work
- The framework prioritizes aligning AI **governance across sectors**, tackling issues like privacy, competition, and innovation
- Regular meetings and joint initiatives foster **cooperation between agencies**, ensuring consistent responses to AI risks
- This approach **connects regulators and policymakers**, balancing priorities while maintaining consistent oversight

Netherlands
Department for Coordination of Algorithmic Oversight (DCA)

- The Netherlands' **Digital Regulation Cooperation Platform** links agencies like the **Data Protection Authority** and **Dutch Central Bank** through the **AI & Algorithm Chamber**
- Managed by the **Department for Coordination of Algorithmic Oversight** (DCA), it holds regular meetings, risk reviews, and compliance plans for the AI Act
- **Funding** grows from €1 million (2023) to €3.6 million by 2026, boosting institutional capacity
- The platform **focuses on technical alignment**, enabling agencies to collaborate on AI risks and share expertise systematically

AI Regulation 6/10

AI ACT – Focus on Interconnections with NIST AI RMF

One of the main **challenges** in addressing **AI**'s rising **challenges** is the feasibility of designing **harmonized** and **interoperable frameworks**. **EU AI Act** and **NIST AI RMF** are examples of how **different frameworks** could focus on **tackling similar challenges** in **AI governance** showing a concrete example of how regulatory efforts can be **integrated** to foster responsible **AI development globally**. In particular, the **4 cores** detailed in the **NIST AI RMF** could be **traced back** to specific **AI Act Articles** that embed their logic and concepts.

NIST AI RMF

Govern

Establishes **AI governance** to ensure **responsible AI** development, **deployment**, and **management** through structured **policies** and **risk frameworks**

- **Art.9** RM Systems
- **Art.10** Data Governance
- **Art.15** Accuracy, Robustness Cybersecurity
- **Art.17** QMS

AI Act

- **Art.25** Respons. AI Value Chain
- **Art.41** Common specification
- **Art.42** Presumption of Conformity
- **Art.72** Post-Market Monitoring
- **Art.73** Repo. of Serious Incident

Map

Establishes the **context** to **frame risks** related to an **AI system** and its **lifecycle** consists of many **interdependent** activities involving a **diverse** set of **actors**

- **Art.4** AI Literacy
- **Art.9** RM Systems
- **Art.10** Data Governance
- **Art.11** Tech. Docu.
- **Art.14** Human Oversight
- **Art.17** QMS
- **Art.25** Respons. AI Value Chain

Measure

It aims to **analyze**, **assess**, and **monitor AI Risks** through **quantitative** and **qualitative** techniques using the **input data** retrieved from the **Map function**

- **Art.9** RM Systems
- **Art.10** Data Governance
- **Art.11** Tech. Docu.
- **Art.13** Transparency on Information to Deployers
- **Art.15** Respons. AI Value Chain
- **Art.72** QMS

Manage

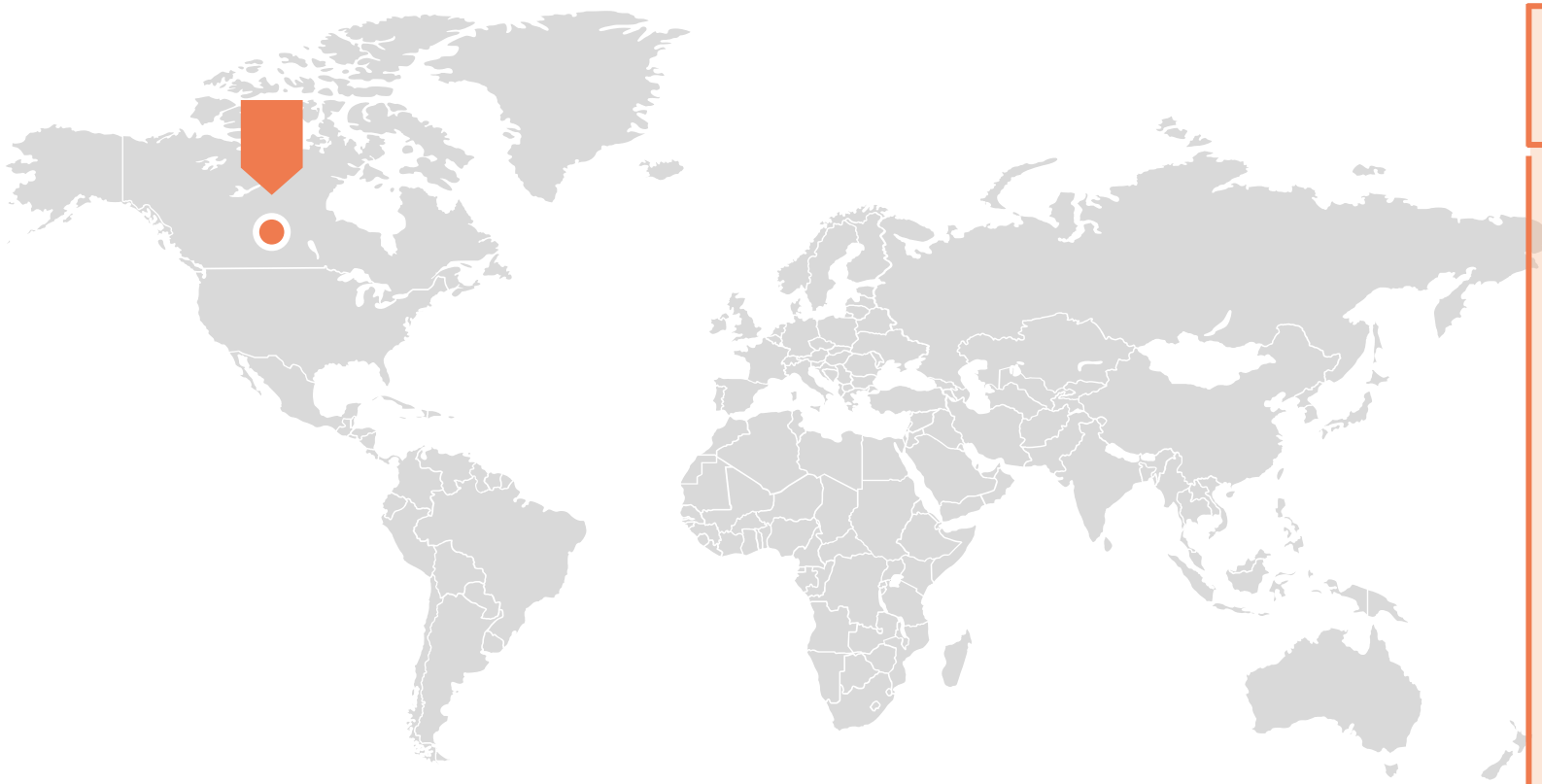
Aims to regularly **allocate risk resources** to **identified** and **assessed risks**, under the **directives** established by the **Govern** function

- **Art.9** RM Systems
- **Art.11** Tech. Docu.
- **Art.14** Human Oversight
- **Art.25** Respons. AI Value Chain
- **Art.72** Post-Market Monitoring
- **Art.73** Repo. of Serious Incident

AI Regulation 7/10

Canada – AIDA and Digital Regulator Forums

Canada's proposed **Artificial Intelligence and Data Act** (AIDA), focusing on transparency and accountability for **high-impact AI systems**, is still **under the national regulatory life-cycle**. **Canada's Digital Regulators Forum**, launched in 2023, aims to strengthen **collaboration across regulatory bodies** to share and oversee on digital markets including the evolution of AI.



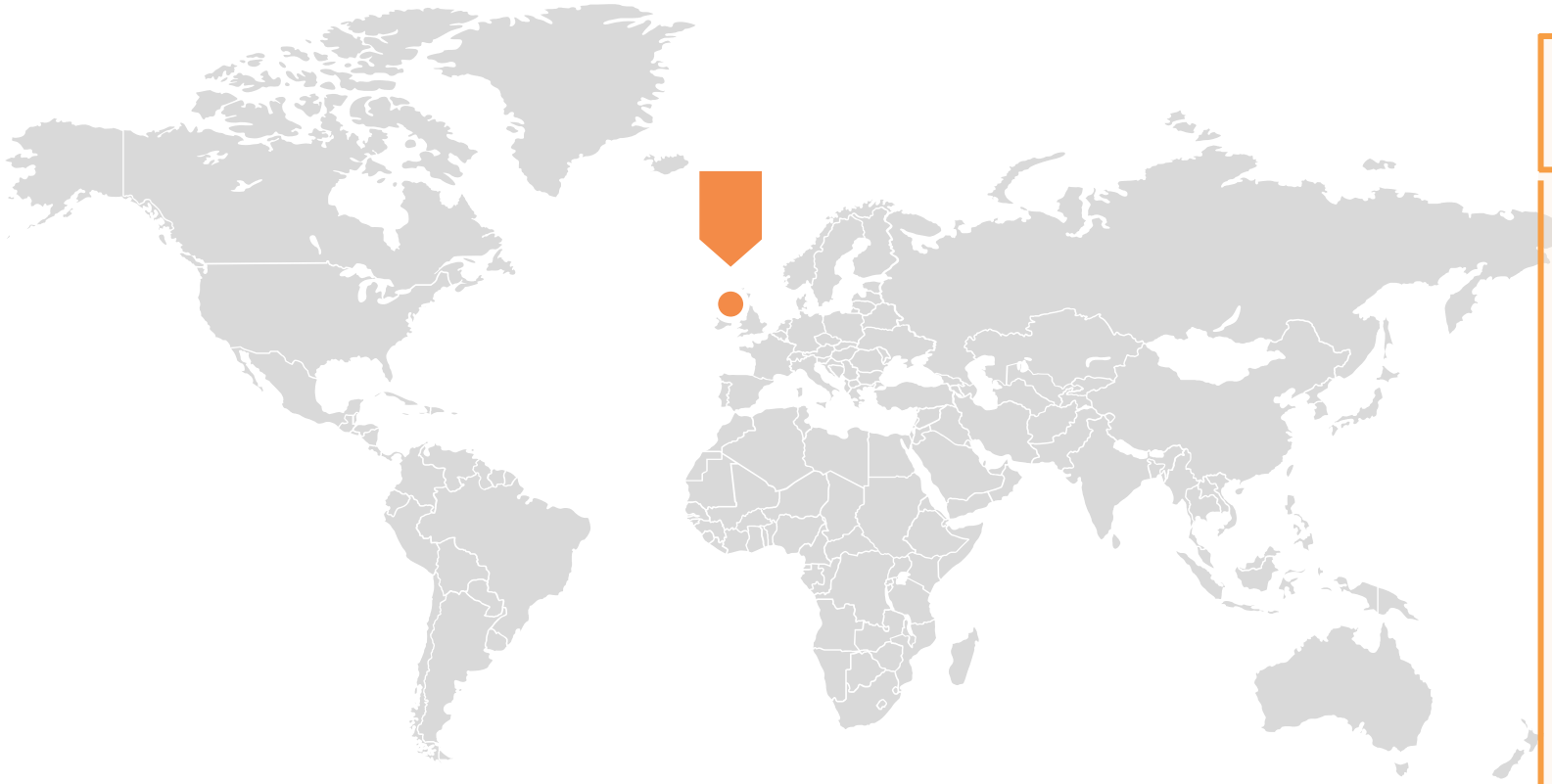
Canada
Digital Regulators Forum

- Canada's **Digital Regulators Forum** connects agencies like the **Competition Bureau** and **Privacy Commissioner**
- Launched in 2023, it **promotes joint research**, information sharing, and flexible responses to AI challenges
- Flexible, *ad hoc* participation allows **adaptability** to emerging issues
- The forum prioritizes **cohesive oversight** of digital markets, addressing **privacy**, **competition**, and **consumer rights**
- **Cross-agency** efforts bridge gaps between regulations, ensuring consistent enforcement and balanced innovation

AI Regulation 8/10

UK – Digital Regulation Cooperation Forum

The UK follows a **principles-based**, **sector-led**, **non-statutory approach**, empowering **existing regulators** to **oversee AI** use within their domains promoting pro-innovation and international interoperability, while gradually building centralized support. In 2021, the **Competition** and **Markets Authority**, the **Information Commissioner's Office**, the **Office of Communications**, and the **Financial Conduct Authority** established the **Digital Regulation Cooperation Forum** to build a **collaborative approach** to **oversee** digital technologies including **AI.**



United Kingdom
Digital Regulation Cooperation Forum

- **UK**'s **Digital Regulation Cooperation Forum** (DRCF) **unites regulators** (e.g. Information Commissioner's Office, Financial Conduct Authority) to coordinate AI governance
- The **Bank of England's AI Consortium** (launched in 2024) **partners with private firms** to study AI risks and draft best practices
- The UK-led **International Network for Digital Regulation Cooperation** (INDRC) globally shares domestic regulatory strategies
- Focus areas include **financial stability**, **consumer protection**, and **innovation**
- Regular collaboration ensures **aligned oversight**, **reducing fragmentation** and supporting secure AI integration

AI Regulation 9/10

Australia – Digital Platform Regulators Forum

Australia has **not yet defined** a **specific regulatory framework** focused entirely on **AI** but has introduced specific voluntary frameworks regarding **AI Ethics Principles** (2019) and **AI Safety Standards** (2024). In 2021, the **Australian Competition** and **Consumer Commission**, the **Australian Communications** and **Media Authority**, the **Office of the Australian Information Commissioner**, and the **e-Safety Commissioner** established the **Digital Platform Regulators Forum** to **coordinate regulation**, **policy** and **enforcement** regarding digital platforms and emerging technologies, including **AI.**

Australia
Digital Platform Regulators Forum

- Australia's **Digital Platform Regulators Forum** (DP-REG) **connects bodies** (e.g. Competition Commission, e-Safety Commissioner) to tackle AI risks
- Established in 2021, it **harmonizes oversight** across competition, privacy and online safety
- **Focused on large tech firms**, the forum coordinates enforcement, aligns mandates and strengthens institutional capacity
- Regular dialogue **ensures unified responses to AI-driven threats**, balancing innovation with public safety

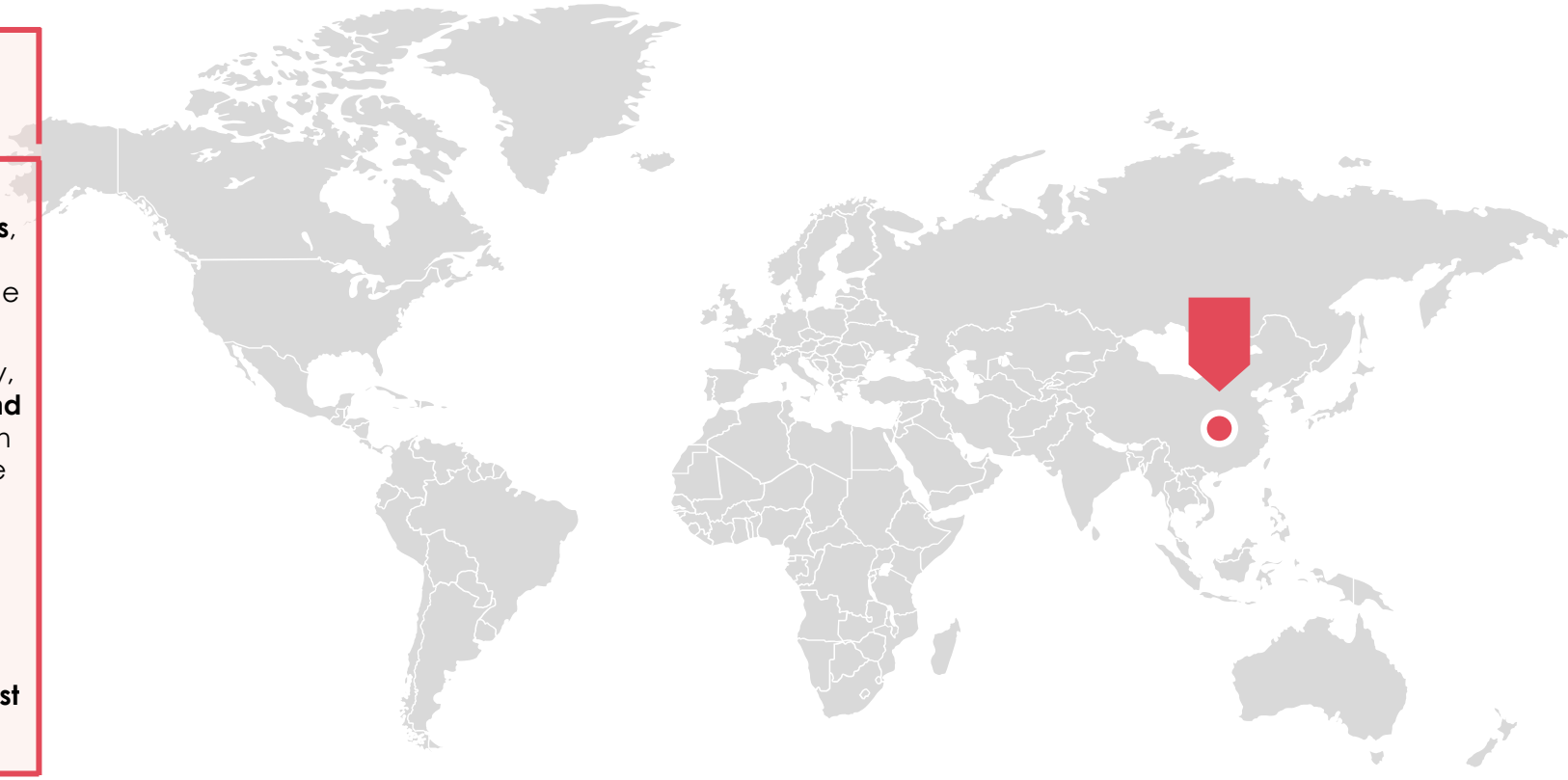
AI Regulation 10/10

China Approach

China's approach to AI regulation is centered around strong **government oversight**, focusing on ethics, data control, and national security. The government has introduced risk-based guidelines and frameworks for **high-impact AI** applications.

China

- China's AI governance is built on **multiple laws**, including the **Personal Information Protection Law** (PIPL), the **Data Security Law** (DSL) and the **Artificial Intelligence Service Regulations**
- **PIPL** and **DSL** ensure **data privacy** and security, regulating **how AI models handle personal and sensitive data**. **AI Service Regulations** focus on **ethical AI development**, ensuring compliance with national security requirements
- **Strict government oversight** ensures AI aligns with national interests
- Unlike the **EU's risk-based** approach or the regulatory strategies in the UK, Australia, and Canada, China takes a **top-down**, **security-first stance on AI governance**



04

Conclusions

How to Assess AI Regulatory Challenges

Conclusions

How to Assess AI Regulatory Challenges

Despite recent regulatory advances, several critical challenges, such as global fragmentation, ethical risks and real-time oversight, remain **insufficiently addressed**, requiring new tools, stronger enforcement, and international coordination.

Challenges		Solutions
Many regulations (e.g. AI Act, DSA) suffer from slow rollout and limited enforcement. **Regulatory capacity** remains **uneven**, especially in developing countries	**Enforcement**	Accelerate **institutional support**, create public appeal channels and **simplify compliance** for smaller actors
Existing regulations are mostly **regional**, leading to **inconsistent** standards **across borders**. Developing countries and SMEs face barriers to compliance and AI adoption	**Global Fragmentation**	Promote **international treaties**, **mutual recognition systems** and capacity-building support **for lower-resource regions**
Foundation models and generative AI are **not fully captured** by current rules. AI models continue to evolve post-deployment, while **monitoring mechanisms are static**	**Evolving AI Technologies**	Introduce **dynamic risk assessments**, model **documentation requirements** and **real time monitoring** obligations
AI applications in biometrics, surveillance and emotion recognition raise major ethical concerns. **Social manipulation** and **discrimination risks** remain **underregulated**	**Ethical, social Oversight**	Require **ethics impact assessments**, strengthen bans on sensitive AI uses and empower ethics review bodies

ESSENTIAL SERVICES FOR FINANCIAL INSTITUTIONS

iason is an international consulting firm that has been supporting both financial institutions and regulators in topics related to Risk Management, Finance and ICT since 2008

Strategy

Strategic advisory on the **design** of **advanced frameworks** and **solutions** to fulfil both **business** and **regulatory needs** in Risk Management and IT departments

Methodology & Governance

Implementation of the designed **solutions** in bank departments **Methodological support** to both **systemically important financial institutions** and **supervisory entities**

Solution

Advanced **software solutions** for **modelling, forecasting, calculating** metrics and **integrating** risks, all on cloud and distributed in Software-as-a-Service (**SaaS**)

KEEP IN TOUCH

iason

Company Profile

iason is an international firm that consults Financial Institutions on Risk Management. Iason integrates deep industry knowledge with specialised expertise in Market, Liquidity, Funding, Credit and Counterparty Risk, in Organisational Set-Up and in Strategic Planning.

Margherita Ranieri

Fabrizio Gentalavigna

This document was prepared in collaboration with Leonardo Bandini and Nicola Mazzoni who at the time were working for Iason Consulting.

www.iasonltd.com