Cambridge Forum on AI: Law and Governance (2025), **1**, e13, 1–17
doi:10.1017/cfl.2024.13

RESEARCH ARTICLE

From principles to practice: The case for coordinated international LLMs supervision

Oscar Borgogno and Alessandra Perrazzelli

Banca d'Italia, Roma, Lazio, Italy
Corresponding author: Oscar Borgogno; Email: oscar.borgogno@bancaditalia.it

The views expressed in this article are those of the authors and do not involve the responsibility of Banca d'Italia and the other institutions which they belong.

(Received 24 October 2024; accepted 12 November 2024)

Abstract

This paper examines the rise of monitoring schemes to coordinate supervisors and market authorities in addressing the cross-industry challenges posed by large language models' deployment. As artificial intelligence (AI) intersects with the core mandate of market authorities dealing with financial stability, data protection, intellectual property, competition and telecommunications, effective oversight requires collaboration and information sharing. Using examples such as the Canadian Digital Regulator's Forum, the UK's Digital Regulation Cooperation Forum and the European Union's AI Act implementation process, the paper illustrates how national and international institutional coordination can help operationalizing the high level principles on AI governance which are currently discussed in international fora. Ultimately, this approach aims to ensure responsible AI development while addressing risks and maximizing its societal benefits.

Keywords: regulatory coordination; competition; data protection; telecommunication; financial stability

1. Introduction: AI's ubiquity and the need for institutional expertise

Large language models (LLMs) are widely expected to revolutionize industries and deliver aggregate macroeconomic productivity growth, unlocking unparalleled opportunities while introducing complex legal and regulatory challenges (OECD, 2024a, 2024b). To fully understand the significance of this development, we must first recognize its growing omnipresence in today's economy and society. Recent data reveal a surge in artificial intelligence (AI)-related investments, particularly in sectors such as semiconductors. For instance, equity markets have adjusted their forecasts, anticipating strong revenue growth through 2025, with projections indicating a $165 billion increase in semiconductor revenues – roughly 0.6 per cent of U.S. GDP – and a $110 billion boost for AI hardware enablers (Sachs, 2024).

It is important to note that we are still in the early stages of AI adoption. For example, recent declines in the share prices of AI chip producers this past summer have led some to question whether the AI revolution will truly be the game-changer it has been portrayed to be (Floridi, 2024). However, we must distinguish between AI's immediate impact on financial markets and its broader economic influence. While the hype surrounding new technologies can lead to bubble-like behaviour, this should not overshadow the potential long-term economic benefits of AI (Global Economics Update, 2024). In fact, it is likely that the full impact of AI on the economy will take several years to materialize.

Meanwhile, technological advancements continue at a rapid pace. Although we are far from achieving "artificial general intelligence" – which could replicate human intelligence across a wide range of tasks – technology companies are pushing the boundaries of what is possible. OpenAI, for example, recently launched the "Strawberry" models, a platform with enhanced reasoning capabilities aimed at addressing more complex problem-solving tasks.

Despite this optimistic outlook, AI adoption remains relatively modest across industries. Currently, only 5.9 per cent of U.S. firms are using AI to produce goods or services, a slight increase from 4.6 per cent earlier this year (Sachs, 2024). Interestingly, significant variation exists across sectors: while the education and information sectors report increased AI adoption rates, industries such as transportation and manufacturing have seen a decline. This fluctuation raises important questions about the underlying barriers to AI integration and the specific needs of different sectors.

In the financial services sector, the trend of AI adoption is more pronounced. A 2023 survey revealed that over 66 per cent of financial institutions employing AI do so primarily for data analytics and back office – making it the most common application in this industry (BIS, 2024a, 2024b). Additionally, the rise of generative AI has not gone unnoticed, with over 40 per cent of financial institutions indicating its use, demonstrating a growing interest and application among industry leaders. The global generative AI market in finance is projected to grow at a staggering compound annual growth rate of 28.1 per cent from 2023 to 2032, with estimates suggesting an increase from $1.09 billion to approximately $9.48 billion within that timeframe (Statista, 2024).

It is often the case that technology-driven industries – ranging from international telecommunications regulations to financial systems and pharma – require effective government oversight to address technology-related risks (Bengio et al., 2024). For instance, regulatory frameworks in the pharmaceutical industry ensure that new drugs are safe and effective, thereby building public trust and promoting further responsible innovation. AI is no different in this regard; it requires tailored supervisory mechanisms to oversee its potential for autonomous action, explosive progress, adversarial threats and irreversible damage. At the same time, AI safety research currently struggles to keep pace with the rapid development of AI technologies. As the scale and complexity of risks associated with AI continue to grow, market agencies and policymakers might find themselves lacking the right tools and expertise to cope with the challenges brought by AI across the economy.

Against this background, at the international level, a range of initiatives is setting major building blocks for AI governance. The Recommendation of the OECD Council on Artificial Intelligence (the "OECD AI Principles"), adopted in May 2019 and updated in May 2024, provides the first intergovernmental set of AI principles, designed to remain robust amidst evolving policy and technological landscapes. These principles are meant to influence global policy, forming the basis of the 2019 G20 AI Principles, and today guide efforts across regions, including the European Union (EU), Council of Europe and United Nations, as well as several national governments (OECD/UNESCO, 2024). As countries embed values-based principles into AI legislation, standards and regulations to ensure policies are suited for trustworthy AI, the influence of the OECD AI Principles is evident worldwide, including in Canada, Egypt, Italy, Japan, Korea, the UK, the U.S. and the EU. These principles advocate for AI that is innovative, trustworthy and aligned with democratic values, calling on governments to engage with stakeholders to ensure AI's benefits are broadly and equitably shared.

Furthering ethical AI governance, UNESCO's Recommendation on the Ethics of AI, adopted in 2021, stands as the first global standard in AI ethics. This framework ensures that AI systems are designed, developed and deployed to respect human rights, support diverse and inclusive societies and promote sustainable development throughout the AI lifecycle. Beyond setting forth values and principles, the Recommendation identifies 11 key policy areas for member states, urging the implementation of governance frameworks and institutional mechanisms to monitor the ethical impacts of AI across its lifecycle. Recognizing that countries vary widely in AI readiness, UNESCO's approach advocates for international cooperation, sharing best practices and fostering collective advancements in ethical AI.

https://doi.org/10.1017/cfl.2024.13 Published online by Cambridge University Press

Complementing this, UNESCO's Readiness Assessment Methodology (RAM) enables countries to evaluate their readiness to develop and govern AI technologies responsibly. The RAM encompasses qualitative and quantitative assessments of key AI ecosystem dimensions, including legal, regulatory, social, cultural, economic, educational and infrastructural aspects.

In September 2024, the UN's High-Level Advisory Body on Artificial Intelligence released its final report, outlining a global blueprint for AI governance (UN, 2024). This report emphasizes the need for a globally inclusive and distributed architecture for AI governance through international cooperation. It proposes seven recommendations to bridge existing gaps, urging governments and stakeholders to work collectively to ensure AI fosters human rights and drives inclusive development. Light yet agile institutional mechanisms are suggested to enhance global AI governance and adapt to AI's rapid evolution.

As such, this article emphasizes that developing shared principles at the international level is insufficient if national implementation is left unchecked. Different legislative interpretations and enforcement practices, even when based on common objectives, can lead to elevated legal uncertainty for market participants and inadequate cross-border protections for individuals if coordination and institutional expertise are lacking.

Given the rising need for legal harmonization in AI governance to mitigate economic frictions in global trade and reduce burdens on operators and consumers alike, there is a clear need for jurisdictions to align their approaches to AI-enabled risks (Fritz & Giardini, 2024). The challenges of reaching consensus on common AI regulations among major geopolitical blocs remain significant, especially in today's international context (Aaronson, 2024). Given the complexities of global relations, a comprehensive international agreement on AI is unlikely in the near future (Aaronson, 2024). Therefore, it is crucial to ensure that market authorities are aligned and "speak the same language" to address, at least in part, the root causes of international legal heterogeneity, which can adversely affect both market players and consumers in digital markets (Huq, 2024).

Similar to the challenges faced in transnational data governance, where the Joint Statement Initiative on E-commerce at the World Trade Organization (WTO) encountered significant setbacks regarding cross-border data flows (Gao, 2024), conflicting national priorities are hindering the creation of a cohesive global regulatory framework for AI. Some countries prioritize rapid AI development to gain a competitive edge and build a national industry that will not jeopardize their national security (as seen in the U.S.), while others focus on social control (as in China) or emphasize human rights and safety, as in the EU (Borgogno & Matteo, 2024). This diversity of approaches highlights the urgent need for a common understanding among global enforcers and market supervisors to address AI-enabled risks, which, like all aspects of the digital economy, will inevitably have cross-border impacts. However, market authorities may lack the mechanisms and expertise necessary to prevent misuse and reckless behaviour, not to mention the ability to coordinate with their peers at the international level.

In light of the above, this contribution focuses on the potential and limitations of structural collaboration among market authorities – those public entities responsible for implementing existing regulations and new ones which have been tasked to enforce new AI-safety legal frameworks. Given that legislators are currently not well positioned to harmonize their laws, it makes sense to explore the degree to which market supervisors can share expertise both domestically and at the supranational level to minimize institutional overlaps and inconsistencies in exercising their mandates.

This article is structured as follows: Section 2 illustrates how, in this current time of uncertainty regarding the impact of AI, market authorities have taken centre stage in addressing this pressing issue. Section 3 explains why, in the case of AI and technology frontiers more generally, it is essential that market authorities do not act in silos. Section 4 examines the most advanced national and international initiatives aimed at regulatory coordination among market authorities. Section 5 presents the case for bottom-up coordination, asserting that effective governance necessitates coordinated cross-border efforts to build institutional expertise, dispel misconceptions, foster innovation and align global safety priorities. Section 6 concludes.

https://doi.org/10.1017/cfl.2024.13 Published online by Cambridge University Press

2. The challenge for market authorities

Supervisors and market authorities are called upon to anticipate the amplification of ongoing harms, as well as to identify new risks, preparing for potential threats long before they materialize. This proactive approach is essential to safeguard the well-functioning of markets and protect consumers from harm (Ranchordas & Vinci, 2024).

However, while it is imperative for regulatory agencies to maintain vigilance and act effectively, they often encounter constraints that limit their operational capacity. As a result, these agencies are compelled to prioritize their core institutional tasks over exploratory endeavours related to emerging technologies. Consequently, it is impractical for each authority to tackle the multifaceted challenges posed by AI independently. Such an approach risks creating legal unpredictability and redundancy, given AI's pervasive impact across multiple industries and the entire economy.

Moreover, market authorities frequently lack both the necessary mechanisms and the expertise to effectively prevent misuse or reckless behaviour in the AI domain. The magnitude of the risks associated with AI necessitates that governance initiatives evolve to become more anticipatory in nature. Indeed, financial supervisors and competition enforcers are increasingly expected not only to react to harms as they arise but also identify and mitigate potential threats before they come to fruition. This shift from reactive to proactive enforcement is critical to maintaining the stability of financial markets and competition in highly innovative markets.

As such, for market authorities, engaging with AI is a complex and multifaceted task. The monitoring challenge is compounded by the fact that malfunctioning or abuses related to AI may unfold with unprecedented speed and intensity, exceeding the response capabilities observed in past market disruptions. This is why to remain effective overseers, authorities must not only address AI-driven risks but also harness AI technologies in pursuit of their own regulatory objectives.

Further, market authorities and government agencies find themselves at a significant disadvantage when compared to the private sector, particularly in the realm of AI. Private financial institutions possess superior expertise, enhanced computational resources and, increasingly, access to vast quantities of high-quality data. AI engines operating in the private sector benefit from robust intellectual property (IP) protections and proprietary data, both of which are often out of reach for regulatory bodies. This disparity in resources and capabilities makes it challenging for supervisors to fully comprehend, monitor and mitigate the risks posed by AI technologies.

In a worst-case scenario, the knowledge gap between regulators and market participants could embolden the latter to engage in increasingly aggressive risk-taking, operating under the assumption that regulatory intervention is less likely due to the authorities' limited oversight capabilities. This situation could not only jeopardize workable competition and efficiency of markets but also erodes public trust in regulatory frameworks designed to ensure market integrity and protect consumers.

Additionally, given the speed at which AI-driven crises can develop, the establishment of coordination schemes that can be triggered instantly will be crucial in pursuing effectively public objectives. For instance, by forming public–private partnerships and establishing AI-to-AI communication links, regulatory authorities can benchmark the performance of private-sector AI applications, conduct stress tests and simulate responses to potential crises (Biancotti, Camassa, Coletta, Giudice & Glielmo, 2024). These schemes could provide rapid responses to emerging threats, thereby safeguarding against potential systemic risks that could otherwise escalate rapidly. Moreover, although the pace and extent of AI adoption remain uncertain, there is a need to avoid a scenario where policymakers are forced to choose between allowing a powerful new technology to threaten market functioning or restricting its use and forfeiting growth and innovation – simply due to a lack of regulatory frameworks that enable its safe integration.

Of course, successfully executing their public mandate – whether through the establishment of public–private partnerships or the development of effective regulatory frameworks – requires a high level of institutional expertise. Without this core pool of know-how, regulators risk becoming outpaced and unable to deal with the very market players they are meant to oversee.

https://doi.org/10.1017/cfl.2024.13 Published online by Cambridge University Press

Therefore, it is essential that market authorities invest in coordinating between themselves and building best practices.

3. The global need for coordination among market authorities

The increasing complexity of AI technologies and their implications for various sectors necessitates a shared monitoring scheme that unites supervisors and regulatory bodies (Adriana, 2023). Such coordination is essential to develop best practices, facilitate knowledge exchange and avoid the pitfalls of acting in silos, which can lead to regulatory fragmentation and inefficiencies.

As noted by Pablo Hernández de Cos, the former Governor of the Bank of Spain and now the newly appointed General Manager of the Bank of International Settlements, achieving high-level convergence and trust in AI supervision hinges on effective coordination and sustained information-sharing efforts among different authorities (de Cos Pablo, 2024). This call for collaboration is particularly urgent in light of the profound transformations AI is set to bring to the financial services landscape and beyond.

One of the primary areas where coordinated efforts are necessary is the distribution of financial services, which is set to be impacted by large-scale AI data analytics coupled with personal data sharing in Internet of things (IoT) environments (BIS (Bank for International Settlements), 2024a). This topic intersects with the responsibilities of various market authorities: financial supervisors, due to potential implications for financial stability and exploitation of retail consumers (Leitner, Singh, Kraaij & Zsámboki, 2024); IP offices as both the models and the training materials could be covered by copyright, patents or sectorial IP protection (Gervais, 2024); data-protection authorities, as it involves the systematic exploitation of personal data (OECD, 2024); competition agencies, considering the potential for collusion and exclusionary behaviours by firms with market power (Bostoen, 2024); and telecommunication authorities, given its reliance on access to internet infrastructure (European Commission, 2024).

In summary, the need for a global framework of coordination among market authorities has never been more pressing. By fostering collaboration across financial, IP, data protection, competition and telecommunications sectors, regulators can develop a cohesive strategy to manage the complexities and risks associated with AI. This collective effort is not only meant to enhance the effectiveness of regulatory responses but also promote innovation and safeguard public interests in an increasingly interconnected digital economy.

Establishing this framework requires commitment and leadership from market authorities to share information, best practices and insights. It will also necessitate the development of common standards and guidelines that can be adopted across jurisdictions. In an era where AI transcends borders, regulatory coherence is essential for ensuring that market participants operate under a unified set of supervisory best practices, thereby minimizing legal uncertainty and fostering a more predictable environment for investment and innovation.

At this stage of the analysis, it is important to explore why AI presents inherent complexities that, if not addressed in a coordinated manner, could render public oversight ineffective. Issues such as value chain concentration, AI explainability and vulnerabilities to cyberattacks overlap with the mandates and concerns of various market authorities. This makes coordination and structured dialogue essential for effectively leveraging public resources. The following subsections offer a brief overview of why this is the case with reference to the mandate of specific authorities.

3.1. Financial stability supervisors

The financial sector has a well-established history of pioneering technological adoption, from the introduction of ATMs to the latest advancements in AI. This trend places the financial industry at the forefront of addressing the challenges associated with frontier technologies. The rapid evolution of AI, particularly through advanced AI agents capable of autonomous decision-making, introduces new layers of complexity. As these systems increasingly integrate into core financial functions, ensuring effective human oversight becomes more difficult, raising significant concerns for financial stability and intersecting with broader supervisory issues (Danielsson & Uthemann, 2024).

While AI brings benefits such as improved operational efficiency, enhanced regulatory compliance, personalized financial products and advanced data analytics, it also has the potential to amplify certain vulnerabilities within the financial sector, thereby increasing systemic risks (Financial Stability Board, 2024). Several AI-related risks are particularly noteworthy.

First, 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.

Second, the widespread use of common AI models and datasets could lead to increased correlations in trading, lending and pricing activities. This uniformity heightens the potential for amplified market stress, exacerbated liquidity crunches and greater asset price vulnerabilities. Additionally, the concentration of resources – intellectual, computational and data-driven – required to develop advanced AI models has resulted in an oligopoly among top providers (Shabsigh and Boukherouaa, 2023). Recent surveys indicate that nearly half of third-party AI models in use come from the three leading providers. This concentrated reliance poses macro-level risks: disruptions to foundational models or their supporting cloud infrastructure could have systemic consequences, while correlated responses across institutions could intensify market stress during economic turbulence.

Third, the increasing adoption of AI raises the risk of cyberattacks by malicious actors. The intense use of data, novel interaction methods with AI services and dependence on specialized service providers expand the avenues for potential attacks. This growing exposure increases both the frequency and impact of cyber threats (OECD, 2023).

Fourth, the complexity and limited explainability of some AI models make assessing their quality and reliability challenging. This is particularly true for foundation models trained on vast datasets far exceeding traditional scales. Ensuring alignment with regulatory standards becomes increasingly difficult as biases or low-quality data embedded in these models are harder to detect and address (Bommasani et al., 2022).

Given that these issues span the mandates of authorities overseeing data security, competition policy and telecommunication infrastructure, it is crucial to ensure their actions are aligned to address their potential impacts on the financial sector effectively.

3.2. *Data protection authorities*

AI technologies, including generative AI, rely heavily on the processing of personal data, which raises significant concerns regarding privacy, bias and discrimination (G7, 2023). These risks exist even when personal data are not directly processed, as AI systems can perpetuate unfair processing and discrimination, potentially influencing broader societal dynamics through the creation of deep fakes and the spread of disinformation. As a result, the protection of personal data and the right to privacy have become more crucial than ever. 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 (lukács & Váradi, 2023).

Data protection authorities have long played a pivotal role in AI governance by leveraging their extensive experience to address AI-related issues. They contribute through the development of recommendations, guidelines, policy documents and enforcement actions.[1]

[1] Internationally, data protection agencies collaborate through various fora, including (1) The Global Privacy Assembly, which has adopted key resolutions on big data, ethics in AI, facial recognition technology and generative AI systems; (2)

https://doi.org/10.1017/cfl.2024.13 Published online by Cambridge University Press

Given the complexity of AI technologies, which often involve the large-scale collection of personal data and the use of sophisticated algorithms, data protection authorities have emerged as central figures in AI governance. They bring their deep expertise in data protection to the forefront, ensuring that privacy and ethical standards are upheld as AI technologies evolve. Their role is indispensable in fostering "trustworthy" AI, ensuring that these technologies are developed and used responsibly. By drawing on their extensive experience and working in collaboration with stakeholders, data protection authorities can navigate the intricate legal and ethical issues surrounding AI, promoting its lawful development while safeguarding human rights.

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 generative AI. Data protection authorities are also actively monitoring technological advancements by engaging with stakeholders, producing reports, discussion papers and guidelines to address these issues. Additionally, they contribute to the development of AI-specific governance by drafting opinions on legislative initiatives. Collaborative efforts with other regulators through regulatory sandboxes allow for testing and evaluating AI technologies in controlled environments. Furthermore, compliance investigations into AI providers help assess how personal data are managed throughout the development and deployment of AI models.

Education is another critical area where data protection agencies play a significant role. By engaging with both public and private sector stakeholders, they help raise awareness of AI technologies and their safe exploitation. This ongoing effort to educate the public equips individuals and organizations with the knowledge they need to navigate the evolving AI landscape responsibly.

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 inherently cross-border nature of AI requires a coordinated international effort to ensure that privacy and data protection standards are upheld consistently, ensuring consumer trust in the digital economy.

3.3. IP offices

As AI systems continue to evolve, IP offices and enforcement agencies face a myriad of challenges and opportunities in establishing effective IP policies tailored to these technologies (Frosio, 2023). AI and Machine Learning (ML) systems can be protected under traditional IP frameworks, primarily through copyright and patent law. However, the Convention on the Grant of European Patents (EPC) as in force since 13 December 2007 specifies that only computer-implemented inventions can be patented, not software per se. This distinction raises critical questions about what constitutes patentable subject matter in AI technologies. Furthermore, drafting claims that satisfy the disclosure requirements for AI inventions poses a significant challenge. As IP offices navigate these complexities, they must address novel issues related to the patentability of innovations, including how the doctrine of equivalents applies to AI inventions (World Intellectual Property Organization, 2024).

AI's reliance on vast datasets for training raises questions about data ownership and IP rights in these inputs. IP offices must consider who owns the IP in the datasets used to train AI systems and whether new IP rights should be created to protect intermediate data generated during this process. Additionally, the intersection of data protection regulations, such as the EU General Data Protection Regulation, with IP law is vital for ensuring compliance as AI systems evolve.

The International Working Group on Data Protection in Technology, which has published working papers on privacy and AI, "smart cities" and large language models; (3) The Association francophone des autorités de protection des données personnelles (AFAPDP), which adopted a resolution on AI development; (4) The Red Iberoamericana de Protección de Datos, which issued recommendations on AI data processing; (5) Ongoing discussions within the Asia Pacific Privacy Authorities (APPA) on privacy and AI.

https://doi.org/10.1017/cfl.2024.13 Published online by Cambridge University Press

The creative outputs generated by AI – such as datasets, art, music and literature – challenge existing copyright frameworks. Questions surrounding authorship, originality and ownership of AI-generated works are pressing and could impact the activity of other market authorities (for instance, competition and financial regulation supervisors). For instance, should AI be recognized as an author under current copyright laws? How should IP offices address potential copyright infringement by AI systems that produce works based on existing materials? Moreover, the impact of AI-generated creativity on cultural diversity and identity necessitates careful consideration in policymaking.

AI's capacity to innovate raises fundamental questions regarding inventorship and patentability. If an AI system independently invents a product or process, who should be recognized as the inventor? IP offices need to develop frameworks that can adequately address these questions, ensuring that innovations resulting from AI processes are eligible for protection under existing patent laws.

Further, the rapid advancement of AI technologies brings challenges to enforcers, as a protectionist approach that prioritizes the profit maximization of IP rights holders (primarily incumbent big tech firms) can hinder dynamic competition and limit public access to information and culture (Ghidini, 2024). Developing effective IP policies requires a comprehensive understanding of the unique issues posed by AI and ML systems, including data ownership, innovation and enforcement mechanisms. In order to address these questions in an industry-sensitive fashion, IP offices needs to interact with other market authorities and make sure their action is aligned with overarching public policy objectives.

3.4. Competition agencies

Competition authorities play a vital role in directing the evolving landscape of AI. As AI-driven markets grow, the risks of collusion and exclusionary behaviours threaten fair competition across the economy (van der Veer & Bostoen, 2024). These authorities are now expected to effectively monitor market dynamics and enforce regulations to prevent anti-competitive practices, ensuring that the benefits of AI technologies are accessible to all participants (Hofmann & Lorenzoni, 2023).

Traditionally, competition authorities have focused on ensuring compliance with competition laws in highly concentrated tech-industries. They have been traditionally active in identifying potential anti-competitive issues, particularly concerning vertical relationships between large digital firms and new comers. For instance, agreements like Google's pre-installation of its AI model "Gemini Nano" on devices raise concerns about limiting access to other foundation models.

The European Commission is also scrutinizing partnerships, such as that between Microsoft and OpenAI, from a merger control perspective (Kowalski, Volpin, and Zombori, 2024). Although initial findings suggested that Microsoft did not gain lasting control over OpenAI, the authority continues to monitor similar arrangements, including significant employee transfers, like Microsoft hiring much of Inflection's workforce (Michal & Rubinfeld, 2023). Such transfers may require assessment under EU merger rules, especially if they result in significant market position changes in generative AI.

Defining relevant markets in the AI sector is complex and should be part of thorough investigations. Insights from first empirical analysis suggest differentiating between upstream markets, which may include AI developers acquiring data, cloud capacity or talent, and downstream markets focused on selling generative AI services. As the industry is still nascent, alternative metrics for assessing market shares, such as usage volume and processing capacity costs, may be necessary.

Market definitions should also consider network effects and ecosystem dynamics (Martínez, 2024). The risk that dominant players might restrict access to key generative AI components could undermine competition. Strategies like exclusivity agreements or self-preferencing can distort competition, limiting consumer choice.

Additionally, competition authorities must be vigilant regarding horizontal agreements that might reduce competitive constraints or facilitate the unlawful exchange of sensitive information. Vertically

https://doi.org/10.1017/cfl.2024.13 Published online by Cambridge University Press

integrated players might adopt pricing policies that disadvantage other market participants, leading to anti-competitive dynamics. There is also the risk of “killer” acquisitions aimed at eliminating nascent competition, which could harm innovation and consumer choice (Tzanaki, 2023). While partnerships between large companies and small AI developers can foster competition, they also risk concentrating key inputs among a few players, necessitating ongoing scrutiny from competition authorities to maintain a fair playing field.

The enforcement of competition policy across different sectors influences how risks related to concentration, collusion, parallel behaviours, cybersecurity and correlation impact financial supervisors, data protection agencies, IP offices and telecommunication authorities. This speaks to the importance of fostering dialogue and collaboration among these public entities to address competition challenges effectively.

3.5. Telecommunication authorities

Telecommunication authorities must play a central role in the evolving dialogue surrounding AI integration, as the effectiveness of AI applications is heavily dependent on a robust and reliable internet infrastructure (BEREC (Body of European Regulators for Electronic Communications), 2023). The increasing interconnectivity of AI, the IoT and telecommunications amplify the importance of network reliability; any vulnerabilities in telecommunications infrastructure can directly impair AI system performance across the economy. A coordinated and strategic approach is necessary to address these infrastructure challenges and facilitate the seamless adoption of AI technologies across various sectors.

The deployment of AI systems relies on several critical enablers, including access to large quantities of reliable data, sufficient storage and processing capacity, and robust electronic communication network connectivity. Additionally, emerging technologies, such as cutting-edge computing architectures, are expected to unlock AI’s full potential by improving its accessibility and performance. However, uneven access to these essential enablers may create disparities among players in the development and implementation of AI. Standardization, therefore, plays a key role in reducing time to market, lowering development costs, promoting interoperability and fostering a level playing field. It also enhances market surveillance, reduces lock-in effects and supports innovation (Borgogno & Colangelo, 2023).

The benefits AI can bring to the telecommunications sector are significant. AI technologies can reduce operational costs by automating complex or repetitive tasks, optimizing network operations, improving customer service and detecting new business opportunities. Moreover, AI can facilitate the expansion and densification of network infrastructure. When properly applied, AI can also enhance energy efficiency within networks, contributing to both cost savings and positive environmental impacts through reduced energy consumption.

The widespread adoption of AI will likely influence the design of telecommunications networks. This could entail new hardware requirements and the integration of diverse hardware and software components. Cloud-based AI systems, for instance, may require low-latency environments, potentially leading to a decentralization of data centre distribution. Furthermore, AI systems operating alongside IoT infrastructure – where numerous devices are connected to a single system – may increase network load, especially in the event of a malfunction.

Telecommunications market players predict that the adoption of AI-driven operational procedures will become standard within the next six to ten years. Many of the network changes driven or enabled by AI, such as network virtualization, are expected to revolutionize not only how networks operate but also their fundamental capabilities. AI will likely automate network resource management while ensuring the customer experience of users.

The potential uses of AI extend to public telecommunication authorities themselves. These authorities could harness AI to improve processes related to policymaking, public service delivery and

https://doi.org/10.1017/cfl.2024.13 Published online by Cambridge University Press

internal management. Although some telecommunications regulators have begun to examine the use of AI within the industry, few have explored how AI could be integrated into their internal operations.

As AI becomes more prevalent, telecommunication authorities must not only understand the risks associated with AI but also develop effective methods for monitoring and assessing these risks in alignment with the mandates of financial supervisors, competition authorities and data protection agencies.

4. An overview of current initiatives and the role of international fora

As different market authorities are called to monitor AI development, a range of initiatives is slowing emerging globally to foster coordination among them. This section highlights some of the most significant efforts, showcasing how these initiatives are paving the way for cohesive regulatory frameworks that address the multifaceted risks associated with AI.

4.1. Main national efforts and the International Network for Digital Regulation Cooperation

Outside the EU, a diverse array of initiatives has emerged across various jurisdictions to facilitate institutional dialogue on AI governance. The UK plays a leading role in advancing both domestic and cross-border regulatory efforts. By promoting a pragmatic approach, the UK advocates for the establishment of a coordinated monitoring scheme at both domestic and international levels, setting the groundwork for comprehensive AI oversight across jurisdictions. A prominent model in this realm is the Digital Regulation Cooperation Forum (DRCF), designed to foster sustained dialogue and regulatory coordination among market supervisors. The DRCF unites key UK supervisory bodies, including the Information Commissioner's Office, the Competition and Markets Authority, the Office of Communications and the Financial Conduct Authority (FCA). Together, these bodies facilitate cross-sectoral regulatory efforts, and similar frameworks are gaining traction in Australia and the Netherlands. These models provide valuable blueprints for other nations striving to establish cohesive supervisory structures not only for AI but also for broader cross-industry risks characteristic of the digital economy.

The Bank of England has further advanced the UK's regulatory landscape by establishing an AI Consortium on 25 September 2024, comprising private sector stakeholders and AI experts, to study AI's potential benefits and examine varied risk management approaches currently in use. This consortium seeks to establish best practices for mitigating financial stability risks and to assess whether additional regulatory guidelines are necessary to secure safe AI integration. The Bank's Financial Policy Committee will provide a detailed evaluation of AI's impact on financial stability and outline ongoing risk monitoring strategies. Working closely with the FCA, the UK government and international regulators, the Bank of England aims to support a secure AI integration, maximizing its potential for economic growth.

On the other side of the Atlantic, Canada has also made strides in digital regulation through the establishment of the Canadian Digital Regulators Forum in June 2023, which involves the Canadian Radio-television and Telecommunications Commission, the Competition Bureau, the Office of the Privacy Commissioner of Canada and the Copyright Board of Canada. This Forum promotes information sharing and collaborative efforts on digital markets and platforms, allowing members to exchange best practices, conduct research and collaboratively address regulatory challenges. Additional Canadian agencies may join on an ad hoc basis, expanding the forum's capacity for addressing emergent issues as they arise.

In Australia, the Digital Platform Regulators Forum (DP-REG) was formalized in March 2022, bringing together the Australian Competition and Consumer Commission, the Australian Communications and Media Authority, the eSafety Commissioner and the Office of the Australian

https://doi.org/10.1017/cfl.2024.13 Published online by Cambridge University Press

Information Commissioner. Through DP-REG, members address cross-cutting issues such as competition, consumer protection, privacy, online safety and data security. This forum illustrates how regulatory cooperation can respond to the complex challenges posed by large multinational digital entities, harmonizing competition, privacy and consumer protection efforts to address the intersecting issues within the digital regulatory space.

These international efforts reflect a shared need among regulators to tackle common challenges, such as safeguarding consumer protection, fostering innovation while ensuring public safety and addressing the market dominance of powerful digital platforms. Collectively, these models try to fill the institutional gap in AI governance through coordination frameworks that adapt to the rapid evolution of AI and digital technologies across borders.

Finally, such national initiatives are now sparking cross-border dialogue, with the UK taking the lead in fostering collaboration and sharing domestic experiences. In June 2023, the UK DRCF expanded its international reach by launching the International Network for Digital Regulation Cooperation (INDRC), which builds relationships with global regulators and enhances domestic cooperation within jurisdictions. INDRC serves as a platform for discussions on maintaining coherence across digital regulations, allowing members to exchange insights on regulatory consistency in various contexts. During the inaugural INDRC meeting in June 2023, the DRCF hosted representatives from similar bodies, such as Australia's DP-REG, the Netherlands' Digital Regulation Cooperation Platform (SDT) and Ireland's Digital Regulators Group (DRG). The meeting agenda featured presentations on the DRCF's objectives and SDT's transparency initiatives. A second INDRC meeting in January 2024 continued this collaborative approach, focusing on members' responses to AI regulatory challenges and the practicalities of information sharing across coordination platforms.

Additionally, on 8 November 2024, the INDRC co-hosted a workshop with the OECD to explore the intersections of various regulatory domains in the context of emerging digital innovations. The workshop highlighted the benefits of interagency collaboration for producing coherent regulatory responses and enhancing public trust.

4.2. The EU: between homogenous regulation and decentralized implementation

The EU is advancing towards a comprehensive regulatory framework for AI with the introduction of the AI Act, the first set of rules worldwide aimed at AI safety. Scheduled to take effect on 1 August 2024, the AI Act marks a significant milestone in the EU's regulatory landscape. Notably, this Regulation envisions that competent authorities responsible for supervising and enforcing EU financial services legal acts may be designated, within their existing competences, to oversee its implementation unless member states decide otherwise.[2] This role includes market surveillance of AI systems used or provided by regulated financial institutions, as well as notifying the European Central Bank (ECB) of any relevant information identified during these market surveillance activities that may benefit the ECB's prudential supervision tasks.

Further, to address regulatory coherence with respect to big tech governance, the High-Level Group of EU regulators – covering consumer protection, competition, data protection and audiovisual media – issued a public statement on 22 May 2024, reaffirming their commitment to aligning AI development with the objectives of the Digital Markets Act (DMA). While preliminary, this statement indicates a promising step towards greater institutional coordination across the EU's various regulatory bodies.

In the Netherlands, the Dutch Data Protection Authority established the Department for the Coordination of Algorithmic Oversight (DCA) to focus specifically on coordinating algorithmic oversight. In October 2021, the Digital Regulation Cooperation Platform was launched, bringing together the Netherlands Authority for Consumers and Markets, the Dutch Authority for the

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (Text with EEA relevance), OJ L, 2024/1689, Recital 158, Article 74(6)-(7).

Financial Markets (AFM), the Dutch Data Protection Authority (AP) and the Dutch Media Authority (CvdM) to collaborate on overseeing digital services.

The DCA hosts the AI & Algorithm Chamber, an administrative consultation body within the Digital Regulation Cooperation Platform. This Chamber works closely with the Authority for Digital Infrastructure to prepare for monitoring compliance with the AI Act.

The AI & Algorithm Chamber includes institutional participation from eight oversight authorities, functioning on three levels: daily work and cases, department heads and directors, and board members. Its operations involve regular and ad-hoc meetings, with physical meetings held twice a year (lasting 2–3 hours) and online meetings occurring more frequently (1–1.5 hours). Since its establishment in July 2023, the Chamber has already held 10 meetings focusing on cases and themes such as technical developments, AI Act oversight and implementation and broader oversight experiences.

The Chamber also engages in monitoring and preparing risk reports, providing input and final approval before publication. Additionally, the DCA advises ministries on structuring Dutch market surveillance and developing frameworks for collaboration. Since 2023, the DCA has received €1 million in funding, with plans to increase this amount incrementally to €3.6 million by 2026.

As coordinating authorities, the Authority for Digital Infrastructure and the Data Protection Authority recommended on 17 November 2024 that the new AI market surveillance authorities, such as Dutch Central Bank and the Dutch AFM, collaborate by sharing domain-specific insights and coordinating responses to emerging risks (Data Protection Authority and Authority for Digital Infrastructure, 2024).

Inspired by Dutch and British models, France has taken notable steps to strengthen regulatory coordination in the digital sector. Acknowledging the challenges posed by overlapping responsibilities among regulators, the country has created a forum to foster collaboration among agencies governing the digital economy. The *Law Aiming to Secure and Regulate the Digital Space*, enacted on 21 May 2024, integrates the DMA and Digital Services Act into French law. Under Article 51, this law establishes a "national coordination network for the regulation of digital services" designed to enhance alignment between agencies overseeing digital services.

This network will include key regulatory authorities such as the Regulatory Authority for Audiovisual and Digital Communication, the Data Protection Authority, the Electronic Communications, Postal and Print Media Distribution Regulatory Authority, the Competition Authority (*Autorité de la Concurrence*), the National Agency for Information Systems Security and the Authority for the Social Relations of Work Platforms. Adding a unique dimension, the framework also involves government departments such as the Ministries of Justice, Interior, Education, Health, Foreign Affairs, Culture and Economy, Finance, and Industry, ensuring comprehensive coverage of relevant sectors.

The structure of the French cooperation entity consists of two interdependent levels. At the steering-body level, the Network of Digital Regulators convenes every four months, bringing together the Minister for Digital Affairs, presidents of regulatory authorities and directors-general from various ministries. This group focuses on formal exchanges, setting the strategic roadmap and identifying key discussion topics. Supporting this political body, a technical group operates at a more granular level, meeting monthly to provide specialized expertise and detailed policy analyses. This group includes directors, heads of units and policy officers from the regulatory agencies and ministries.

The overarching aim of this mechanism is to create a collaborative platform that addresses regulatory challenges spanning multiple agencies' competencies, fosters the sharing of best practices to enhance inter-agency dialogue and establishes robust feedback loops between policymakers and independent regulators. These efforts are intended to improve regulatory outcomes by bridging gaps in communication and expertise.

The network is set to address a range of pressing topics, including the deployment and trustworthiness of AI models, competition issues and the role of public–private partnerships. Other focal points include navigating the balance between crime prevention, privacy rights and encryption integrity,

https://doi.org/10.1017/cfl.2024.13 Published online by Cambridge University Press

developing practical regulatory tools such as compliance frameworks and guidelines, interpreting the country-of-origin principle in digital regulation and refining methodologies for conducting risk assessments. Through these initiatives, the French coordination framework aims to position itself at the forefront of digital governance.

Ireland has bolstered its regulatory cooperation by establishing the DRG in 2022. This group brings together the Commission for Communications Regulation (ComReg), the Data Protection Commission, the Competition and Consumer Protection Commission and Coimisiún na Meán (CnaM). The initiative aims to adopt a whole-of-government approach to the digital agenda, focusing on identifying areas of regulatory commonality and challenges, ensuring the consistent and cohesive application of digital legislation, maximizing the coherence of digital and regulatory structures and supporting a broader framework for regulatory cooperation.

The DRG's first significant output is the *Digital Skills Report*, which addresses the critical need for institutional regulatory expertise. The report emphasizes the importance of attracting and retaining top-tier senior professionals with specialized digital skills, alongside the appropriate aptitude and attitude, to effectively manage responsibilities across the digital legislative landscape. To enhance the sourcing strategies of DRG members, the report outlines a range of approaches, including "Buy, Borrow, Bot, Bind, Build, and Bolster," and highlights the importance of a clearly defined and fully implemented employee value proposition.

In Italy, Article 18 of the Draft Law on AI, presented to Parliament on 20 May 2024, mandates a coordinated framework for implementing the AI Act.[3] The Italian Cybersecurity Agency and the Agency for Digital Italy (Agenzia per l'Italia Digitale, AgID) are tasked with coordinating these efforts across public authorities. Furthermore, a coordination committee, comprising the director-generals of relevant authorities, is to be established within the Presidency to promote regulatory alignment and cooperation.

4.3. The G7 Agenda and global initiatives

At the international level, existing institutions such as the UN Secretary-General's AI Advisory Body and the OECD have emerged as crucial platforms for facilitating global dialogue on the risks associated with AI diffusion. These institutions, along with specialized agencies like the WTO, World Intellectual Property Organization (WIPO) and the International Telecommunication Union (ITU), which organizes the AI for Good Global Summit, provide essential infrastructure for structured international cooperation. Their expertise in IP policy and technical standards can be leveraged to develop guidelines for responsible AI innovation and deployment, helping national policymakers worldwide expand their understanding of AI's complexities and implications.

Furthermore, the G7's efforts to convene experts and assess the potential evolution of AI and its economic risks are promising steps towards enhancing cross-border policy awareness. Building on the Hiroshima Process's International Guiding Principles for Advanced AI Systems, which establish key standards – fairness, accountability, transparency and inclusiveness – the G7 has taken a leading role in advocating for regulatory coordination.[4] Further, during their meeting in Rome on October 4, representatives from G7 competition authorities and policymakers highlighted the need for collaboration among regulators and enforcement agencies, emphasizing the significance of cross-agency deliberations to address the multifaceted challenges posed by AI (Roundtable of G7 Data Protection and Privacy Authorities, 2024).

[3] Senato della Repubblica Italiana, Disegno di Legge presentato dal Presidente del Consiglio dei Ministri e dal Ministro della giustizia, Comunicato alla Presidenza 20 maggio 2024, Disposizioni e delega al Governo in materia di intelligenza artificiale, https://www.senato.it/service/PDF/PDFServer/DF/437373.pdf.

[4] This non-exhaustive list of guiding principles was discussed and elaborated as a living document to build on the existing OECD AI Principles in response to recent developments in advanced AI systems and are meant to help seize the benefits and address the risks and challenges brought by these technologies. See: https://www.mofa.go.jp/files/100573471.pdf.

https://doi.org/10.1017/cfl.2024.13 Published online by Cambridge University Press

5. The case for bottom-up coordination in market supervision

The implications of large-scale AI data analytics, particularly in the context of personal data sharing within IoT environments, raise the institutional need for such coordination. As showed in previous sections, various market authorities – ranging from financial supervisors to IP offices, data protection authorities, competition agencies and telecommunication authorities – share responsibilities that intersect significantly in this arena. Financial supervisors are tasked with safeguarding financial stability and consumer protection, while IP offices must navigate copyright and patent issues related to AI models and training materials. Data protection authorities play a crucial role in managing personal data risks, competition agencies are vigilant against potential collusion and exclusionary behaviours and telecommunication authorities ensure the necessary internet infrastructure is in place. Thus, continuous and structured dialogue among these public bodies is essential to address the multifaceted challenges AI poses within their respective mandates.

To ensure that adequate expertise is developed on the field, it is key that such a monitoring scheme works both at the domestic as well as at the international stage, paving the way for coordinated AI oversight among as many countries as possible. This is why we argue for a bottom-up approach to AI monitoring activities, starting at the domestic level (Perrazzelli, 2024). By establishing robust national frameworks that ensure sustained dialogue and coordination between market supervisors, countries can develop institutional expertise and ensure a whole-of-government response, while laying the groundwork for international understanding.

Strengthening coordination and shared expertise within jurisdictions also facilitates meaningful dialogue at the transnational level, particularly among regulators from like-minded regions such as the UK and the EU (Borgogno, Perrazzelli, 2024). Despite differing regulatory approaches – such as the UK's light-touch regulatory stance on AI safety – there exists an opportunity for mutual understanding and the exchange of supervisory best practices. This collaborative dialogue is crucial, given the shared values and regulatory standards that underpin both jurisdictions in areas like financial regulation and data protection.

Furthermore, the role of existing international institutions, such as the UN Secretary-General's AI Advisory Body and the OECD, is pivotal in facilitating global discussions on AI risks (United Nations, 2024). These organizations, along with specialized agencies like the WTO, BIS, WIPO and the ITU, provide essential frameworks for structured international cooperation. By leveraging their expertise in trade governance, IP policy and technical standards, they can assist in formulating guidelines for responsible AI innovation and deployment, thus enhancing national policymakers' understanding of AI's evolving dynamics.

The utilization of AI models opens up new opportunities for market authorities in pursuit of their policy objectives. A consistent theme throughout this section has been the importance of data as a critical prerequisite for the successful application of machine learning and AI. Effective data governance frameworks will be integral to any successful AI application. Market authorities' policy challenges, therefore, encompass both the models and the data they utilize. An important trade-off arises between using "off-the-shelf" models versus developing in-house, fine-tuned versions. While employing external models may be more cost-effective, especially in the short run, and leverages the comparative advantages of private sector companies, it also introduces challenges related to transparency and dependence on a limited number of external providers. Beyond the general risks that market concentration poses to innovation and economic dynamism, the high concentration of resources could create significant operational risks for market authorities, potentially affecting their ability to fulfil their mandates.

Another crucial aspect relates to market authorities' roles as users, compilers and disseminators of data. Market authorities rely on data as a vital ingredient in their decision-making processes and communication with the public. They have historically served as extensive compilers of data, either collecting it independently or drawing from other official agencies and commercial sources.

https://doi.org/10.1017/cfl.2024.13 Published online by Cambridge University Press

Additionally, market authorities are also providers of data, serving both governmental entities and the general public. This role helps them fulfil their obligations as key stakeholders in national statistical systems. The rise of machine learning and AI, alongside advances in computing and storage capacity, has intensified the urgency of these roles. Market authorities must now analyse and utilize increasingly large and diverse sets of structured and unstructured data, often held by the private sector. Although LLMs can assist in processing such data, issues like hallucinations or prompt injection attacks may lead to biased or inaccurate analyses.

In recent years, the costs of commercial data have surged, and vendors have imposed stricter usage conditions. The decision regarding whether to use external or internal models and data carries far-reaching implications for market authorities' investments and human capital. A key challenge lies in establishing the necessary Information Technology (IT) infrastructure, which becomes more complex if market authorities choose to develop internal models and collect or produce their own data. Providing adequate computing power and software, alongside training existing personnel or hiring new staff, entails substantial upfront costs. The same holds true for creating a data lake, which involves pooling various curated data sets. A reliable and secure IT infrastructure is not only crucial for big data analysis but also essential for preventing cyberattacks.

Hiring or retaining personnel with the appropriate mix of economic understanding and programming skills presents its own challenges. As AI applications evolve and become more sophisticated, the demand for personnel with the right skills will only increase. Survey-based evidence suggests that this concern is particularly pronounced among market authorities. There is a high demand for data scientists and other AI-related roles, but public institutions often struggle to compete with private sector salaries for top AI talent. Additionally, the need for staff with the right skills arises from the limitations associated with using AI models to assist in monitoring financial stability, as previously discussed. Ultimately, AI cannot replace human judgment; it requires oversight by experts with a solid understanding of macroeconomic and financial processes.

In brief, there is an urgent need for market authorities to collaborate in fostering the development of a "community of practice" dedicated to sharing knowledge, data, best practices and AI tools. In light of rapid technological change, exchanging information on policy issues arising from the role of market authorities as data producers, users and consumers is imperative for developing effective regulatory frameworks that safeguard the public interest while fostering innovation in AI applications.

6. Conclusion

This contribution has examined the potential and limitations of structural collaboration among market authorities tasked with monitoring and supervising AI-based services. As the landscape of AI technology evolves at an unprecedented pace, the existing regulatory frameworks must also adapt to address the associated risks and challenges. However, given the current limitations faced by legislators in achieving harmonization in laws (Jamshidi, 2023), it becomes imperative to explore the role of market supervisors in sharing expertise both domestically and at the supranational level to partially address the economic and social costs arising from global legal heterogeneity.

Overall, the rapid and widespread adoption of AI implies that there is an urgent need for market authorities to raise their game. To address such new challenges, market authorities need to upgrade their capabilities both as informed observers of the effects of technological advancements as well as users of the technology itself. As market observers, authorities need to stay ahead of the impact of AI on economic activity through its effects on aggregate supply and demand. As users, they need to build expertise in incorporating AI and non-traditional data in their own analytical tools. Market authorities will face important trade-offs in using external vs internal AI models, as well as in collecting and providing in-house data vs purchasing them from external providers.

https://doi.org/10.1017/cfl.2024.13 Published online by Cambridge University Press

Together with the centrality of data governance, the rise of AI will require a rethink of market authorities' traditional roles as compilers, users and providers of data. To harness the benefits of AI, collaboration and the sharing of experiences emerge as key avenues for market authorities to mitigate these trade-offs, in particular by reducing the demands on information technology infrastructure and human capital. Market authorities need to come together to form a "community of practice" both at the domestic and cross-border level to share knowledge, data, best practices and AI tools.

As we move forward, it is essential for market authorities to engage in continuous dialogue and develop frameworks that promote coordinated efforts across jurisdictions. By leveraging existing international institutions and collaborative initiatives, it is possible to create a more robust regulatory environment that balances innovation with safety and accountability. Indeed, it is not enough that countries agree on high level principles if then they are translated into domestic regulation or implemented in heterogeneous forms. This diversity highlights the urgent need for a common understanding among regulators and market supervisors to address AI-enabled risks, which, like all aspects of the digital economy, will inevitably have cross-border impacts.

References

Aaronson, S. A. (2024). The age of AI Nationalism and its effects. CIGI Papers No. 306.

Adriana, D. V. (2023). Coordinating digital regulation in the UK: Is the Digital Regulation Cooperation Forum (DRCF) Up to the task? *International Review of Law, Computers & Technology*, *37*(2), 128–146. doi:10.1080/13600869.2023.2192566

Bengio, Y. et al. (2024). Managing extreme AI risks amid rapid progress. *Science – Policy Forum*, *384*(6698), 842–845.

BEREC (Body of European Regulators for Electronic Communications). (2023). Report on the impact of Artificial Intelligence (AI) solutions in the telecommunications sector on regulation. Retrieved December 18, 2024, from https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-impact-of-artificial-intelligence-ai-solutions-in-the-telecommunications-sector-on-regulation.

Biancotti, C., Camassa, C., Coletta, A., Giudice, O., & Glielmo, A. (2024). Chat Bankman-Fried: An Exploration of LLM Alignment in Finance. On file with authors.

BIS (Bank for International Settlements). (2024a). Annual economic report. Retrieved December 18, 2024, from https://www.bis.org/publ/arpdf/ar2024e.htm.

BIS (Bank for International Settlements). (2024b). Digitalisation of Finance. Retrieved December 18, 2024, from https://www.bis.org/bcbs/publ/d575.pdf.

Bommasani, R., Hudson, D., Adeli, E., & Altman, R. (2022). On the Opportunities and Risks of Foundation Models. Retrieved December 18, 2024, from https://arxiv.org/abs/2108.07258.

Borgogno, O., & Colangelo, G. (2023). Shaping interoperability for the internet of things: The case for ecosystem-tailored standardisation. *European Journal of Risk Regulation*, *15*(1). doi:10.1017/err.2023.8

Borgogno, O., & Matteo, S. Z. (2024). Chinese data governance and trade policy: From cyber sovereignty to the quest for digital hegemony? *Journal of Contemporary China*, *33*(148), 578–602.

Borgogno, O., & Perrazzelli, A. (2024, August 24). A bottom-up proposal for coordinated international AI supervision. Retrieved December 18, 2024, from https://www.promarket.org/2024/08/24/a-bottom-up-proposal-for-coordinated-international-ai-supervision/.

Bostoen, F., & van der Veer, A. (2024). Regulating Competition in Generative AI: A Matter of Trajectory, Timing, and Tools. *Concurrences*. N° 2-2024 – AI & Antitrust.

Danielsson, J., & Uthemann, A. (2024). How Financial Authorities Can Respond to AI Threats to Financial Stability. *VoxEU*, *1* (2).

Data Protection Authority and Authority for Digital Infrastructure. (2024, November 17). Third Advice on the Supervisory Structure for the AI Act. Retrieved December 18, 2024, from https://www.autoriteitpersoonsgegevens.nl/en/documents/third-advice-on-the-supervisory-structure-for-the-ai-act.

de Cos Pablo, H. (2024, April 17). Managing AI in banking: Are we ready to cooperate? In *Keynote speech at the Institute of International Finance Global Outlook Forum*, Basel Committee speeches. Washington, DC.

European Commission. (2024, February 2). "How to Master Europe's Digital Infrastructure Needs?" *White Paper*. COM(2024) 81 final.

Financial Stability Board. (2024). The Financial Stability Implications of Artificial Intelligence. https://www.fsb.org/uploads/P14112024.pdf

Floridi, L. (2024). Why the AI hype is another tech bubble. *Philosophy and Technology*, *37*(4), 128. doi:10.1007/s13347-024-00817-w

Fritz, J., & Giardini, T. (2024). Why Global Coordination Is Necessary for Regulating AI. Retrieved December 18, 2024, from https://www.promarket.org/2024/09/11/why-global-coordination-is-necessary-for-regulating-ai/.

https://doi.org/10.1017/cfl.2024.13 Published online by Cambridge University Press

Frosio, G. (2023). Generative AI in Court. In N. Koutras, & N. Selvadurai (Eds.), *Recreating Creativity, Reinventing Inventiveness - International Perspectives on AI and IP Governance*, Routledge.

Gao, H. (2024). The Joint Statement on E-Commerce: Is This Glass Half Empty or Half Full? Retrieved December 18, 2024, from https://www.cigionline.org/articles/the-joint-statement-on-e-commerce-is-this-glass-half-empty-or-half-full/.

Gervais, D. J. (2024). The Heart of the Matter: Copyright, AI Training, and LLMs. Retrieved December 18, 2024, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4963711.

Ghidini, G. (2024). IP and AI – For a balanced, non-protectionist stance. *GRUR International*, *73*(11), 1017–1018. doi:10.1093/grurint/ikae086

Global Economics Update. (2024, September 26).

Goldman Sachs, Report (2024). AI Adoption Tracker 2024Q3.

Hofmann, H. C. H., & Lorenzoni, I. (2023). Future Challenges for Automation in Competition Law Enforcement. *Stanford Computation Antitrust*. Retrieved December 18, 2024, from https://law.stanford.edu/wp-content/uploads/2023/04/hofmann-lorenzoni.pdf.

Huq, A. Z. (2024, March 11). A world divided over artificial intelligence. *Foreign Affairs*, *7*.

Jamshidi, M. (2023). The private enforcement of national security. *Cornell Law Review*, *108*, 739–838.

Kowalski, K., Volpin, C., & Zombori, Z. (2024). Competition Policy Brief - Competition in Generative AI and Virtual Worlds, https://digital-strategy.ec.europa.eu/en/news/commission-publishes-policy-brief-competition-generative-ai-and-virtual-worlds

Leitner, G., Singh, J., Kraaij, A., & Balázs, Z. (2024, May). "The Rise of Artificial Intelligence: Benefits and Risks for Financial Stability." *Financial Stability Review*. Retrieved December 18, 2024, from https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202405_02%7E58c3ce5246.en.html.

lukács, A., & Váradi, S. (2023). GDPR-compliant AI-based automated decision-making in the world of work. *Computer Law & Security Review*, *50*, 105848. doi:10.1016/j.clsr.2023.105848

Martínez, A. R. (2024). Generative AI and the Digital Markets Act on the Rocks. *Kluwer Competition Law Blog*. Retrieved December 18, 2024, from https://competitionlawblog.kluwercompetitionlaw.com/2024/02/05/generative-ai-and-the-digital-markets-act-on-the-rocks/.

Michal, G., & Rubinfeld, D. L. (2023). Algorithms, AI, and Mergers. *Antitrust Law Journal*. Retrieved December 18, 2024, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4469586.

OECD. (2023). Generative artificial intelligence in finance. *OECD Artificial Intelligence Papers*, 9.

OECD. (2024a). AI, data governance, and privacy: Synergies and areas of international co-operation. *OECD Artificial Intelligence Papers*. No. 22. Paris: Author. 10.1787/2476b1a4-en

OECD. (2024b). "Miracle or Myth? Assessing the Macroeconomic Productivity Gains from Artificial Intelligence." *Working Party No. 1 on Macroeconomic and Structural Policy Analysis*. [Forthcoming as an OECD Working Paper].

OECD/UNESCO. (2024, October 15). "G7 Toolkit for AI in the Public Sector." Italian G7 Presidency and the G7 Digital and Technology Working Group.

Perrazzelli, A. (2024, October 23). "Trust-Oriented AI Governance: A Roadmap for Market Agencies." GWU Competition and Innovation Lab Public Series Lecture. Retrieved December 18, 2024, from https://www.youtube.com/watch?v=grIHrYy5IDc&t=262s.

Ranchordas, S., & Vinci, V. (2024). Regulatory sandboxes and innovation-friendly regulation: Between collaboration and capture. *Italian Journal of Public Law*, *1*, 16.

Roundtable of G7 Data Protection and Privacy Authorities. (2024, October 11). Statement on the Role of Data Protection Authorities in Fostering Trustworthy AI.

Shabsigh, G., & Boukherouaa, E. (2023). Generative artificial intelligence in finance: Risk considerations. *IMF Fintech Notes*, *2023*(006), 1. doi:10.5089/9798400251092.063

Statista. (2024). Artificial Intelligence (AI) in Finance – Statistics & Facts. Retrieved December 18, 2024, from https://www.statista.com/topics/7083/artificial-intelligence-ai-in-finance/#topicOverview.

Tzanaki, A. (2023). Dynamism and politics in EU merger control: The perils and promise of a killer acquisitions solution through a law & economics lens. *Antitrust Law Journal*. doi:10.2139/ssrn.4574948

United Nations. (2024). Governing AI for Humanity: Final Report. *High-Level Advisory Body on Artificial Intelligence*. Retrieved December 18, 2024, from https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf.

van der Veer, A., & Bostoen, F. (2024). Two Views on Regulating Competition in Generative AI. *Network Law Review*. Retrieved December 18, 2024, from https://www.networklawreview.org/veer-bostoen-generative-ai/.

World Intellectual Property Organization (2024). Getting the innovation ecosystem ready for AI – An IP policy toolkit. Retrieved December 18, 2024, from https://www.wipo.int/publications/en/details.jsp?id=4711.

Cite this article: Borgogno O and Perrazzelli A. (2025). From principles to practice: The case for coordinated international LLMs supervision. *Cambridge Forum on AI: Law and Governance* **1**, e13, 1–17. https://doi.org/10.1017/cfl.2024.13