Published October 2024

Regulatory implementation and application alongside EU digital strategy

By Isabelle Roccia and Claude-Étienne Armingaud

Launched in 2015, the EU's Digital Single Market Strategy aimed to foster the digital harmonization between the EU member states and contribute to economic growth, boosting jobs, competition, investment and innovation in the EU.

The EU AI Act characterizes a fundamental element of this strategy. By adopting the first general-purpose regulation of artificial intelligence in the world, Brussels sent a global message to all stakeholders, in the EU and abroad, that they need to pay attention to the AI discussion happening in Europe.

The AI Act achieves a delicate balancing act between the specifics, including generative AI, systemic models and computing power threshold, and its general risk-based approach. To do so, the act includes a tiered implementation over a three-year period and a flexible possibility to revise some of the more factual elements that would be prone to rapid obsolescence, such as updating the threshold of the floating point operations per second — a measurement of the performance of a computer for general-purpose AI models presumed to have high impact capabilities. At the same time, the plurality of stakeholders involved in the interpretation of the act and its interplay with other adopted, currently in discussion or yet-to-come regulations will require careful monitoring by the impacted players in the AI ecosystems.

The EU digital strategy and digital decade

The 2015 Digital Single Market Strategy for Europe foresaw a potential 250 billion euros in generated value and called for a "vibrant knowledge-based society." To implement that vision, the European Commission revealed an ambitious legislative program, which included reforming the EU's telecommunications and copyright legislation and simplifying consumer rules for online and digital purchases, in addition to putting the General Data Protection Regulation into force.

To further this initial ambition, given the ever-so-quick evolution of emerging technologies, the Commission proposed its Path to the Digital Decade in September 2021, followed in December 2022 by the European Declaration on Digital Rights and Principles.

These initiatives not only aimed to modernize the EU regulatory landscape but also to create a stance for Europe by setting up a common corpus of EU democratic values in the digital sphere and ensuring the value generated by this dematerialized sphere benefited Europe.

To support this effort, significant EU funding has also been made available to foster the digital transformation, in particular through the Recovery and Resilience Facility at 150 billion euros, DIGITAL Europe at 7.9 billion euros and Connecting Europe Facility 2 Digital at 1.7 billion euros.

While several aspects of this digital strategy appeared as a logical continuation of existing process, e.g. digital resilience in the financial or other critical sectors, see the Directive on Security of Network and Information Systems and Digital Operational Resilience Act below, the topic of AI quickly arose, almost unannounced.

Once generative AI became publicly available, the media coverage of the promises of AI and its rapid adoption led to the full spectrum of reactions from doomsday sayers to utopians.

Although it was a late guest to the EU digital roadmap, the AI Act went through an accelerated adoption process alongside other texts that were previously initiated. This article aims to analyze the regulatory implementation of the AI Act, notably its interplay with these other regulatory frameworks.

A macro view of the AI Act with other elements of the EU digital strategy

While the AI Act aims to regulate AI generally, its ambition was never to regulate exclusively. Indeed, the ubiquity of AI systems facilitates their inclusion in other products and services that are subject to other regulatory frameworks.

This means compliance with the AI Act is incumbent on compliance with other EU regulations, whether they are technology-neutral cross-sector regulations like the GDPR or sector-specific regulations like the DORA. These additional compliance requirements depend on the specific use case in which a given AI system is deployed.

Data protection

The AI Act and GDPR are part of the broader regulatory landscape designed to govern digital technologies and protect individuals in the digital age. While focusing on different aspects of digital technology and the use of both personal and nonpersonal data, these two pieces of regulation interact closely and share common goals. The eagerness with which some EU data protection authorities leveraged the GDPR, e.g., to tackle AI-related investigations and produce guidance, before the adoption of the AI Act illustrates the interplay and partial overlap between these frameworks.

Principles

Many of the foundational principles that inspired the AI Act are common to data protection, including privacy and data governance, transparency and accountability. However, there is undeniable friction between some of the GDPR innate governing principles and the mere nature of AI technology. Data minimization is perhaps the most obvious.

Complementarity

Not all AI systems use personal data as part of their functionalities. Consequently, the GDPR may not always be a relevant framework. However, the massive ensembles of data processing by large language models, especially in the absence of curation, e.g., through web scraping, makes it more than likely that the GDPR will be relevant, as recently demonstrated by the position on LLMs taken by Hamburg's data protection authority, the Commissioner for Data Protection and Freedom of Information. Similarly, while the GDPR does not focus on AI, its Article 22 provisions pertaining to automated decision-making highlight the interplay, overlap, overall complementarity and, at times, conflict between the two. Overall, the GDPR is directly referenced 30 times in the AI Act, far more than any other EU regulation.

Risk-based approach

Both the GDPR and the AI Act employ a risk-based approach, but they categorize and handle risks differently. The GDPR categorizes data processing activities based on the level of risk to the data subjects' rights and freedoms, while the AI Act categorizes AI systems based on the level of risk they pose to safety, fundamental rights and other public interests. While the two risk-based approaches often overlap, and the risk-based approach under the GDPR has been put in question, they may also add to one another.

Impact assessments

Under the GDPR, data protection impact assessments are mandatory for high-risk data processing activities. On the other hand, the AI Act also requires impact assessments but focuses on fundamental rights and the ethical use of AI, evaluating issues such as bias, discrimination and potential harm. Once again, while they may partially overlap in scope and purpose, stakeholders will need to devise templates to address all facets. Ideally, the stakeholders responsible for drafting, implementing and maintaining those impact assessments will be able to leverage their DPIAs to meet some of the fundamental rights impact assessment requirements and either be on the same team or closely work together to avoid discrepancies in the documentation.

Supervision and enforcement

Both the AI Act and GDPR provide for robust supervision and enforcement mechanisms. The AI Act creates new bodies, including the AI office and AI Board, and will rely on a net of national authorities. While, under the GDPR, DPAs have been well established for years in each EU member state, the relevant authorities under the AI Act are still debated, which may ultimately lead to divergences in interpretation and enforcement.

Governance

The intricate nature of the two regulations will make for an even more complex framework. However, it also means many organizations will be able to significantly leverage the privacy tools, processes, structures and culture already in place to inform and build their AI governance.

Cybersecurity

The EU's regulatory framework for cybersecurity, including the DORA, the not-yet-adopted Cyber Resilience Act, the revised NIS2 Directive and the Critical Entities Resilience Directive, along with the AI Act, form a comprehensive strategy to address different aspects of the EU's expectations for digital security and resilience. While each of these pieces has its own focus area, be it specific or general, together they have the overarching goal of creating a safer digital environment within the EU.

- **DORA:** This aims to ensure the EU financial sector can maintain operational resilience with a particular focus on information and communications technology risk management. It sets out requirements for financial entities to establish and maintain preventive measures, detection mechanisms, and strategies to respond to and recover from ICT-related disruptions and threats.
- **CRA:** This aims to encourage a life-cycle approach to connected devices, ensure they are placed on the market with fewer vulnerabilities, and enable users to take cybersecurity into account when selecting and using connected devices.
- **NIS2 Directive:** This updates the scope of the original Network and Information Security Directive by expanding the security and notification requirements to more sectors and types of entities, raising the bar for cybersecurity standards, and strengthening national cybersecurity capabilities. It covers a broad range of critical sectors beyond the financial industry.

Complementary objectives

Each piece of the framework shares the common objective of mitigating risks associated with digital technologies. Where the AI Act focuses on risks specifically associated with AI systems, DORA, CRA and NIS2 target the broader digital ecosystem's stability and security.

Risk management

All four pieces of the framework adopt a risk-based approach, alongside accountability frameworks. Stakeholders will need to demonstrate that they not only mapped the actual or potential risks, including AI, associated to their ICT, infrastructure, products and services as relevant, but that the relevant mitigation efforts have been implemented, notably in view of the evolution of technological progress and the state of the art. In addition, similar to the AI Act, the CRA includes obligations to include cybersecurity risk assessments in the technical documentation of new connected devices placed on the market.

Reporting obligations

All pieces of the framework include obligations to report incidents occurring on the platform and/or device to the relevant authorities. When more than one framework applies, stakeholders will need to consider all reporting obligations. Ideally, the authorities responsible for enforcing the AI Act will coordinate with those responsible for the DORA, CRA and NIS2, especially when dealing with AI systems that fall under the critical infrastructure categories. This will be a familiar notion, as incident notification requirements must be considered under NIS2 and the GDPR among other laws.

Operational resilience

AI systems, especially those used within critical infrastructures, need to adhere to the resilience standards outlined in the DORA and NIS2. This means AI system developers and deployers must ensure their systems can withstand, respond to and recover from cyber threats.

In essence, the AI Act, DORA, CRA and NIS2 form a comprehensive approach to safeguarding the EU's digital ecosystem. They are different pieces of the same puzzle, with each regulation targeting specific challenges but ultimately contributing to the resilience, security and trustworthy adoption of digital technologies, including AI, across the EU.

The harmonized application of these regulations is crucial for ensuring the consistency and effectiveness of the digital single market's security, whether by the relevant stakeholders to not duplicate the compliance effort, or the relevant authorities to ensure enforcement actions are coherent. The failure of a coordinated implementation regime would lead to discrepancies and lack of foreseeability by the stakeholders. Technology developments and the evolution of the threat landscape will also be implementation challenges for organizations. This landscape also leaves some room for organizations to leverage AI technology to strengthen their cybersecurity postures.

The AI Act is expected to work in tandem with the GDPR and other digital regulations to create a comprehensive and cohesive framework for digital technology in the EU. In addition, its compliance mechanisms and enforcement will likely build on the foundational doctrines and interpretations developed over the past years. Stakeholders will need to maintain that broad bird's-eye view of the EU regulatory landscape, as well as any changes in the implementation of its components to ensure continued compliance.

Copyright

The EU last updated its copyright rules in its 2019 Digital Single Market Directive, reflecting the state of the art at the time, so minimal provisions are relevant for AI and machine learning. The directive's Article 4 on text and data mining creates an exception to copyright for text and data mining purposes. In fact, copyright appeared late into the AI Act negotiations at the request of the European Parliament, as co-legislators were zeroing in on obligations for general-purpose AI models. The final text primarily draws from EU copyright law.

Article 53 of the AI Act requires providers of general-purpose AI models to put policies in place to comply with EU copyright law, for example to make sure the training data they use respects copyright. They also need to comply with the reservation of rights pertaining to the TDM exception in the Copyright Directive and seek authorization from the copyright holder when needed.

The same article also requires general-purpose AI model providers to "draw up and make publicly available a sufficiently detailed summary about the content used for training of the general-purpose AI model, according to a template provided by the AI Office."

Putting these requirements in practice in the context of the AI Act will not be straightforward and the AI Office is expected to provide useful guidance to stakeholders in that regard, including to clarify the notion of a "sufficiently detailed summary."

A currently incomplete map of requirements

In addition to the expected guidelines and delegated acts, standards are expected to play a key role in stakeholders' compliance effort, notably to benefit from a presumption of conformity, as in Recital 117 and Article 40 et. seq. of the AI Act.

While the European standardization organizations, comprising the European Committee for Standardization, with the European Electrotechnical Committee for Standardization and the European Telecommunications Standards Institute, are currently working on various sets of standards, the official mandate to adopt harmonized standards may not be issued prior to the publication of the AI Act in the Official Journal of the EU. As such, the publication of finalized harmonized standards will be adopted after stakeholders' compliance efforts have started.

Stakeholders will therefore need to pay close attention to the development and publication of these standards. They should prepare their compliance in advance, the case may be on the basis of the published draft, as they will have a narrow window to ensure alignment with technical specifications and complete their conformity assessments.

A growing risk of divergent interpretations

The AI Act includes compliance requirements at both the pre- and post-market stages of AI system deployment. Its enforcement will be entrusted to one notifying authority and one market surveillance authority in each member state per Article 70 of the AI Act. While the resulting designation may target the same authority, this will not always be the case.

In addition, over the past couple of years, several DPAs in big member states have actively leveraged their GDPR responsibilities to assert their expertise in AI systems and relevance in supervising and enforcing the AI Act. All DPAs expect to have a seat at the table, and some have advocated very strongly to become the lead authority.

Each member state retains full control of these designations, still pending in a majority of countries. The close links between the AI Act and the Market Surveillance Regulation no. 2019/1020, see AI Act Article 74, may tip the balance in favor of the well-established member state infrastructure of market surveillance authorities already in charge of the post-market monitoring regime for products in the EU.

The designation of authorities is not straightforward as neither MSAs, DPAs nor any other existing authority would be the perfect blend. For example, one may argue DPAs are not the most relevant authority because AI may not always involve personal data processing activities. Some member states, like Spain, may choose to create a new authority from scratch.

As a result, and despite the tempering function of the EU AI Board, interpretations of key concepts under the AI Act and its enforcement may follow diverging regime and the regulatory implementation may include discrepancies from one member state to the other.

The AI Act created the AI Office, which will advise and assist the European Commission and EU member states to strive for an EU-wide harmonization as part of its mission. Yet, the AI Act builds on a complex matrix of stakeholders that each bring a variety of expertise, cultural and historical differences, which may be challenging to reconcile and harmonize.

The potentially fragmented interpretation could also lead to more stringent requirements bearing on certain stakeholders in certain jurisdictions.

The look ahead

Following the 12 July 2024 publication of the AI Act, the Commission circulated an updated version of the AI Liability Directive that considers the final content of the AI Act, which aims to provide compensation to victims of damage caused by AI. According to Member of the European Parliament and AI Liability Directive Rapporteur Axel Voss, the recently updated Product Liability Directive contains enough loopholes to justify continued work on the AI Liability Directive. This was reiterated by the Parliament's research service in a study that argues the scope of the AILD proposal should extend to include general-purpose and other high-impact AI systems, as well as software.

In its latest version of the AI Liability Directive, the Commission mostly changed the text's wording to match the AI Act's. However, the Commission's changes to Article 4 of the directive increases the potential responsibility of companies deploying AI systems. As it is currently redrafted, this Article 4 would result in the presumption that companies are liable for damage caused if they do not "monitor the operation of the AI system or, where appropriate, suspend (its) use" or use "sufficiently representative" input data.

While compliance with the AI Act should minimize the risk of exposure to liability under the AI Liability Directive, this companion piece will provide individuals with recourse to compensation for the potential damage resulting from the deployment of AI, as opposed to the regulatory fines under the AI Act. This framework would bring more clarity than stakeholders have seen until now under the GDPR, the enforcement of which remains under discussion before the courts, notably for nonmaterial damages.

Conclusion: The need for self-determination of ecosystems

With so many unknowns in the compliance equation, the AI Act may not provide the stakeholders with the expected regulatory foreseeability, which will be the key to developing competitive AI systems and preserving the EU's fundamental democratic values.

In addition, while the EU welcomes input from the stakeholders when developing normative elements, the compromises that must be reached for a baseline regulatory implementation bearing on all stakeholders may not be conducive of accounting for the specific factors of certain ecosystems.

Yet, like the GDPR, the AI Act may retain an ace up its sleeve with codes of practice and codes of conduct.

In the meantime, stakeholders were also invited by the Commission to provide their input on AI, notably through its:

- Directorate-General for Health and Food Safety, which opened a survey on the deployment of AI in health care.
- Directorate-General for Financial Stability, Financial Services and Capital Markets Union, which ran a consultation to gather input from all financial services stakeholders, including companies and consumer associations. Responses can be submitted until 13 Sept. The consultation was designed for respondents developing or planning to develop or use AI applications in financial services. In particular, the DG FISMA aimed to receive views from financial firms that provide or deploy AI systems.