IN-DEPTH

Artificial Intelligence Law

EUROPEAN UNION

LEXOLOGY

Artificial Intelligence Law

EDITION 1

Contributing Editors

Karen Silverman and **Brinson Elliott**

The Cantellus Group

In Depth: Artificial Intelligence Law is a perceptive global overview of the fast-evolving state of law and practice surrounding artificial intelligence (AI) systems and applications. Focusing on recent developments and their practical implications, it examines key issues including legislative initiatives, government policy, AI risk management principles and standards, enforcement actions and much more.

Generated: January 17, 2024

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information.

LEXOLOGY

Explore on **Lexology**

European Union

Elisabetta Righini and Daphné Van der Eycken
Latham & Watkins LLP

Summary

Introduction

Artificial intelligence (AI) is now part of our everyday lives and the significant beneficial effects that come with it have affected society and industry across a myriad of sectors (inter alia mobility, health, agriculture and environment) in the European Union (EU). In the past, the EU called AI 'one of the most strategic technologies of the 21st century', comparing its revolutionary potential with the steam engine or electricity, and manifesting that AI 'is helping us to solve some of the world's biggest challenges'.[2] AI brings its own challenges, however, as observed recently by Ursula von der Leyen, President of the European Commission (EC), who compared it with the discovery of quantum physics, which brought humanity nuclear energy but also nuclear threat.[3]

Although the EU is admittedly not leading the charge in AI in terms of investments[4-] and, therefore, is unlikely to be the place where AI will see its biggest technological breakthroughs, its political leaders are certainly committed to ensuring that Europeans can safely benefit from this new technology within the boundaries of the full respect of their fundamental rights, including with regard to non-discrimination, data protection and privacy. In particular, the EU hopes to set an international golden standard to influence developments in the field, similar to the global influence it had on data protection with the General Data Protection Regulation (GDPR),[5] which has come to be known as the 'Brussels effect'.[6]

More specifically, and since the adoption of the White Paper on AI,[7] the EU is pursuing an ambitious two-fold objective: to encourage AI development while fostering a human-centric approach, laying the foundations for a safe interaction between individuals and AI technologies in line with EU values and principles. On this basis, the EU is working on shaping the AI industry as of its inception with a far-reaching regulatory proposal, the Artificial Intelligence Act (the AI Act Proposal).[8]

Moreover, the EU seems to be moving towards an all-embracing approach to AI. A number of legislative initiatives are being considered to tackle various aspects of AI, such as the AI Liability Directive[9] and the revision of the Product Liability Directive,[10] which the EC proposed on the same day. In particular, one aim of the former is preventing the emergence of fragmented national adaptations of liability rules to AI, while the latter modernises the existing rules on product liability to address the new challenges of the digital age, including AI.

Year in review

i Technology

The AI industry is developing globally, with regional and local divergence driven mainly by investment, policy and regulatory factors, rather than technical factors. The headline trend of the past year is the proliferation of accessible generative AI systems and, more recently, enterprise integration has emerged as a key technological shift, as the main providers in the enterprise SaaS (software as a service) and PaaS (platform as a service) markets integrate generative AI systems into their core products.

ii Developments in policy and legislation

The most significant recent development in the AI space in the EU remains the EC's proposal for a far-reaching regulation of the AI space: the AI Act Proposal.

On 21 April 2021, the EC proposed this new and long-awaited regulation to the EU co-legislators, the European Parliament (EP) and the Council of the EU (the Council), to harmonise the rules on AI systems applicable in the European internal market. One of the aims of the AI Act Proposal is to enhance the functioning of the internal market through a clear set of rules for the development, marketing and use of AI in compliance with EU values. To this end, the Proposal introduces a technology-neutral definition of AI systems in EU law and adopts a risk-based regulatory approach imposing specific obligations whenever an AI system is likely to pose high risks to safety and fundamental rights. More specifically, the obligations are tailored to the level of risk posed by AI (minimal risk, limited risk, high risk and unacceptable risk).

At the same time, the Proposal is also part of the EU's larger strategy to establish a European Digital Sovereignty, an objective that has become a central, albeit vague and controversial, guiding principle for Europe's leadership and strategic autonomy in the digital field. By building its digital Fortress Europe, the EU hopes to make up for current shortfalls, and seeks to compete with the United States and China in the global race to develop new technologies.[11]

At the time of writing, the two EU co-legislators have reached political agreement on the AI Act Proposal, after having debated the Proposal for almost two years. The Council adopted its own revised version of the AI Act[12] on 6 December 2022, but the EP deliberations proved more heated owing to the technological developments and the need to address generative AI. Indeed, after ChatGPT, an AI-powered language model developed by OpenAI and backed by Microsoft, launched in November 2022, Italy became the first country in the EU to ban the software and launch investigations into OpenAI in respect of alleged violations of EU data protection laws and failure to check the age of its users.[13] Italy later withdrew its ban after OpenAI rectified the alleged data protection issues[14] but the fact remains that, with their temporary block, the Italian authorities had opened the door to a fragmented approach across the EU. This factor prompted the EP to amend the AI Act Proposal specifically to address generative AI and it seems that the agreed text will indeed provide for specific transparency requirements for generative AI. After months of negotiations, the EP finally approved its position[15] on 14 June 2023, which introduces almost 800 amendments to the EC's proposal for the AI Act.

In summer 2023, the AI Act entered the last legislative step, the trilogue of inter-institutional negotiations between the EC, the EP and the Council. Given the huge number of EP amendments, it is expected that the text of the AI Act Proposal will be heavily modified before being finalised. It is only once the positions of the three EU institutions are aligned on all the provisions that the two co-legislators will be able to formally adopt the AI Act into law. At the time of writing, the AI Act has been politically agreed and the text will be finalised over the coming weeks but is not expected to take effect before 2026 for most provisions.

iii Cases

Given the novel widespread use of AI technology, EU case law relating to AI is limited. That said, the Court of Justice of the European Union (CJEU) has assessed the use of AI systems by public authorities in one case, *Ligue des droits humains*,[16] which helpfully illustrates how the EU tries to accommodate the use of AI with respect to EU fundamental values.

This ruling was rendered in the context of a preliminary ruling, in which the Belgian Constitutional Court had asked the CJEU to assess the conformity of the national Belgian law transposing EU laws (including the Passenger Name Record Directive[17] (PNR Directive), the Advance Passenger Information Directive[18] and the Reporting Formalities for Ships Directive[19] with EU law principles and fundamental rights.

The PNR Directive allows passenger information units to (1) process PNR data to identify persons who may be involved in terrorist offences or serious crime so that they are required to undergo further examination before boarding a flight, (2) provide access to and process PNR data to prevent, detect, investigate and prosecute terrorism and serious crime and (3) analyse PNR data to update the criteria that should be used to identify persons who may be involved in terrorism or serious crime.[20] The CJEU noted that these criteria needed to be predetermined and, therefore, considered that the use of AI in self-learning systems (or machine learning) was precluded in this area.[21] The CJEU motivated this finding by explaining that machine-learning AI is able to modify without human intervention or to review the assessment of a process and, in particular, the assessment criteria as well as the weighting of those criteria. Furthermore, the CJEU considered that the opacity that characterises the way in which AI works could make it impossible to understand the reasons why a given programme identified a person as potentially involved in terrorism or serious crime.[22] In those circumstances, the CJEU ruled that the use of AI could deprive citizens of their right to an effective judicial remedy and expose them to discrimination.[23]

This judgment confirms that most EU institutions are aligned on making the use of new AI technology compatible with their citizens' fundamental rights. It also seems to follow logically from citizens' right, already enshrined in the EU data protection framework, to not be subject to a decision based solely on automated processing, including profiling.[24] What is interesting, though, is that, on top of restating privacy and data protection as citizens' rights in AI, this judgment establishes that the use of AI must also be vetted against two other fundamental rights, namely the right to an effective judicial remedy and the right to non-discrimination.

Legislative and regulatory framework

The most relevant EU regulatory initiative is the AI Act Proposal. In this section, we analyse and provide details of its scope, the general approach the Proposal takes to AI, its main obligations, the fines and penalties foreseen, the authorities in charge of its enforcement, and a timeline of the adoption of the legislation and of the enforcement of the legislation.[25]

The most relevant EU regulatory initiative is the AI Act Proposal. In this section, we analyse and provide details of its scope, the general approach the Proposal takes to AI, its main obligations, the fines and penalties foreseen, the authorities in charge of its enforcement, and a timeline of the adoption of the legislation and of the enforcement of the legislation.[25]

i Scope

One of the aims of the AI Act Proposal is regulating the trustworthiness of AI systems placed on the EU market (i.e., supplied to the EU market in the course of a commercial activity, whether in return for payment or free of charge) or whose use affects people located in the EU. In particular, it applies to (1) AI system providers that place AI systems on the market or into service in the EU irrespective of the place of establishment of the providers, (2) users of AI systems located in the EU, and (3) AI system providers and users located in a third country, where the output of the AI system is used in the EU.[26] However, the Council reports that the AI Act would not apply to AI systems used solely for research or for non-professional purposes.[27]

The proposed definition of an AI system, under Article 3(1) of the Proposal[28] is:

> software that is developed with . . . [machine-learning approaches, logic- and knowledge-based approaches or statistical] approaches and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

ii General risk-based approach

The AI Act Proposal groups AI practices into four categories according to a risk-based approach (i.e., differentiating between uses of AI systems that would result in an unacceptable risk, a high risk, a low risk, or a minimal risk).

AI practices that are considered a clear threat to the safety, livelihood and rights of individuals are classified as unacceptable and will be prohibited by the AI Act Proposal.[29]

The AI Act Proposal imposes restrictions and requirements on various AI systems that are deemed a high risk to the health and safety or fundamental rights of individuals and fall within one of the categories identified in the AI Act Proposal, which include (among other categories) AI systems used for the purpose of (1) producing safety components of products subject to third-party *ex ante* conformity assessments, (2) using remote biometric identification in public spaces, (3) recruiting or (4) managing and operating essential public infrastructure networks, such as supply of utilities.[30]

The AI Act Proposal places in the limited-risks category AI systems used for the purpose of interacting with individuals, detecting emotions or determining association with (social) categories based on biometric data, or generating or manipulating content (e.g., deepfakes).[31] Pursuant to the Proposal, providers of such AI systems shall ensure that users are aware that they are interacting with or viewing content generated by an AI system.[32]

AI systems that do not fall into any of the aforementioned three categories are considered to pose minimal risk and no specific requirements are imposed on them.

iii Main requirements and obligations for high-risk AI systems

The AI Act Proposal sets forth a number of requirements with which high-risk AI systems must comply. This entails putting in place adequate risk assessment and mitigation systems,[33] keeping detailed documentation,[34] maintaining appropriate human oversight-[35] and ensuring a high level of robustness, security and accuracy.[36]

Moreover, the Proposal also requires compliance with a number of obligations by providers, product manufacturers, importers and distributors of high-risk AI systems. The following is a non-exhaustive overview of these obligations.

The AI Act Proposal requires providers to implement quality management, quality assurance and verification procedures for AI systems.[37] They are also requested to draw up technical documentation and to carry out conduct conformity assessments (and, as applicable, to affix a CE marking to conforming systems).[38] Moreover, they should also commit to correct risks posed by high-risk AI systems and inform national competent authorities of the risks.[39] Furthermore, manufacturers of products in certain sectors that leverage high-risk AI systems must also comply with these obligations.[40] Providers must also establish and document a post-marketing monitoring system to actively and systematically collect, report and analyse the performance of the high-risk AI system with the AI Act Proposal.[41]

Similarly, importers of high-risk AI systems are required to ensure compliance by providers of high-risk AI systems with the obligations outlined above prior to placing such a system on the EU market.[42]

Before making a high-risk AI system available on the market, distributors must verify that the high-risk AI system bears the required CE conformity marking. They should also check that it is accompanied by the required documentation and instructions for use, and that the provider and the importer of the system, as applicable, have complied with their obligations.[43]

In addition to the obligations described above, which were part of the EC's original Proposal, the co-legislators are reported to have added (1) a requirement to conduct a fundamental rights impact assessment prior to deploying high-risk AI, which is expected to apply to companies providing essential public services, including banks and insurance companies, (2) rights for individuals to submit complaints about AI systems, and (3) rights for individuals to receive explanations about decisions based on high-risk AI systems that impact on their rights.

iv Fines and penalties

In Title X, the AI Act Proposal sets forth tiers of fines that are dependent on the severity of the infringement.

Pursuant to the AI Act, violations concerning prohibited AI practices (Article 5) and the high quality of data used to train AI system (Article 10) will give rise to fines of up to €30 million or 6 per cent of annual worldwide turnover, whichever is higher.[44] Moreover, a violation that amounts to non-compliance with requirements or obligations other than those mentioned above will be subject to fines of up to €20 million or 4 per cent of annual worldwide turnover, whichever is higher.[45]

The supply of incorrect, incomplete or misleading information to regulators in reply to a request gives rise to fines of up to €10 million or 2 per cent of worldwide annual turnover, whichever is higher.[46]

Whenever an AI system does not comply with the obligations and requirement set out in the AI Act, the operators can also be required to take appropriate corrective actions.[47] Other remedies provided for in the AI Act Proposal are withdrawing the AI system from the market or recalling it within a reasonable period.[48]

v Enforcement bodies

The AI Act Proposal foresees a governance system at both EU and national levels.

At EU level, the Act establishes a European Artificial Intelligence Board composed of representatives from the Member States and the EC.[49] The Board will be entrusted with facilitating the effective and harmonised implementation of the rules of the AI Act Proposal in close collaboration with the authorities designated at national level and the EC.[50]

At national level, the AI Act Proposal requires Member States to designate one or more competent authorities, including a national supervisory authority, which would be tasked with supervising the application and implementation of the regulation.[51] National market surveillance authorities would be responsible for assessing operators' compliance with the obligations and requirements for high-risk AI systems.

It is notable that the EP has proposed to simplify this governance system. In particular the EP suggests centralising the AI oversight function in one agency per Member State, which would have stronger enforcement powers, such as requesting access to both the trained and training models of the AI systems, including foundation models. At EU level, the EP proposes to establish an AI Office to supervise the application of the AI Act across Member States, provide guidance and coordinate joint cross-border investigations. In addition, members of the EP are proposing to strengthen citizens' rights to file complaints about AI systems and receive explanations of decisions based on high-risk AI systems that significantly affect their rights.

vi Timing of legislation

Amendments by the EP

The EP made almost 800 amendments to the AI Act Proposal presented by the EC.[52] Among the most significant is the proposal to include a new definition of AI systems that aligns more closely with that of the Organisation for Economic Co-operation and Development and an extended list of AI practices that are prohibited or considered high risk.

Moreover, the EP suggested introducing an extra requirement layer to the high-risk category. More specifically, on the basis of the new set-up, an AI system should be deemed high risk only if it falls within one of the categories identified by the AI Act and poses a significant risk of harm to health, safety or fundamental rights. Therefore, should an AI system provider consider that its system does not pose a significant risk, it could request the relevant regulatory body to exempt it from the obligations applicable to high-risk AI.

Furthermore, the EP focused on some specific obligations to be imposed on generative AI (e.g., ChatGPT), which emerged while the EP was reviewing the EC's proposal: first, these models should be designed and trained to be prevented from generating illegal content;

second, the summaries of copyrighted data used for training them should be published; and third, any content generated by the generative AI should be labelled as 'AI generated'.

The EP is also minded to prohibit the contractual parties in the AI supply chain from contractually reallocating liability for penalties and associated indemnity claims and litigation costs arising under the AI Act.

With reference to the cap for fines imposed on individuals or companies for infringements of the AI Act, the EP suggested €40 million or, if the offender is a company, 7 per cent of the company's worldwide turnover, whichever is higher.

Amendments by the Council

Compared with the EP's Negotiating Position, the Council's amendments appear moderate.[53] Notably, it clarified many of the requirements for high-risk AI systems to make them more technically feasible and less burdensome for stakeholders.

In addition, the Council amended the EC's proposal to account for situations where general purpose AI systems (i.e., those that can be used for many different purposes) are integrated into a high-risk system. In this situation, certain obligations that will be specified in a subsequent text would also apply to general purpose AI systems.

With respect to prohibited practices, the Council suggested extending the prohibition on using AI for social scoring to private actors, and specified the conditions under which the use of AI for law enforcement purposes may be allowed.

Furthermore, the Council introduced increased transparency obligations on high-risk AI systems, such as an obligation for users of an emotion recognition system to inform natural persons when they are being exposed to such a system.

The procedure

Following the adoption by the Council and the EP of their respective negotiating positions, the AI Act entered the last legislative step – the trilogue of inter-institutional negotiations between the EC, the EP and the Council; and the co-legislators reported that they reached a political deal on 9 December 2023. Given the high number of EP amendments, it is expected that the AI Act Proposal will be heavily amended before being finalised. As mentioned above, it is only now that the positions of the three EU institutions are aligned on all the provisions that the two co-legislators will be able to formally adopt the AI Act into law. This is now expected to happen in the first half of 2024. The negotiations have proved to be difficult, however, in particular because the EP wantede to ban AI facial recognition technology, whereas the Council is strongly opposed, given that Member States' governments currently use AI in law enforcement. Based on the co-legislators' press releases, it seems that the agreed position provides for real-time remote biometric identification in narrow circumstances (to prevent terrorist attacks or locate the victims or suspects of a defined list of serious crimes) and *ex post* remote biometric identification strictly in targeted searches for individuals convicted or suspected of a serious crime. In both cases, however, prior judicial authorisation would be required. The EP also wanted to add guardrails for foundational models, whereas the Council says it does not want to hinder innovation and argues that guardrails would go against the aim of the AI Act, which is to regulate risks arising from specific use cases, not the technology itself. It seems that the political agreement subjects both foundational models and general-purpose AI models to transparency requirements, including obligations around technical documentation, compliance with copyright law, and publishing detailed summaries of training data (including copyright protected material). Additional requirements will apply to high-impact foundation models or high-impact general purpose AI involving systemic risk; however, this remains uncertain at present as there are diverging reports from the two co-legislators on this point.

The Council is pushing to have rules in place before the next European elections, which are scheduled for June 2024. Moreover, the competent EC directorate, the Directorate-General for Communications Networks, Content and Technology (Connect), is working in parallel on negotiations for the adoption of standards to apply to AI systems together with the AI Act, and encouraging self-regulation codes in the meantime. On this latter point, Thierry Breton, European Commissioner for the Internal Market, announced on 24 May 2023 that the EC is working on the development of AI Pact, a temporary and voluntary code of conduct to be agreed with European and non-European technology companies developing AI.[54] In early December 2023, compromise proposals circulated among negotiators were pointing to (1) the EC maintaining a list of AI models deemed to pose systemic risk, while providers of general-purpose AI would have to publish detailed summaries of the content used to train them, and (2) free and open-source AI licences being exempted from regulation in most cases, unless, for example, they were deemed at high risk of being used for already banned purposes. However, other critical points, such as the use of AI in biometric surveillance and source code access, had yet to be hashed out.[55] That being said, European initiatives for a temporary AI Pact might become redundant given the introduction of a voluntary code of conduct for AI developers by G7 countries in the framework of the Hiroshima Process.[56]

At this pace, the final text of the AI Act could be adopted before the end of 2023, and surely before the EU elections in June. Once adopted, the AI Act will enter into force one month after its publication in the EU Official Journal. The current proposed text foresees that the majority of the AI Act obligations will take effect two years later (i.e., in mid-2026) at the latest.

Managing AI risks and impacts

To manage the risks posed by AI, the EU is planning to impose obligations with respect to the (1) fairness and (2) transparency of AI systems, while (3) protecting the intellectual property rights of the providers of AI systems. In parallel, the EU contemplates a new regime and an amendment to the current legal framework to (4) ensure that individuals can be compensated for damage caused by AI systems. Finally, the question arises of (5) the geographical scope of any EU regulation.

To manage the risks posed by AI, the EU is planning to impose obligations with respect to the (1) fairness and (2) transparency of AI systems, while (3) protecting the intellectual property rights of the providers of AI systems. In parallel, the EU contemplates a new regime and an amendment to the current legal framework to (4) ensure that individuals can be compensated for damage caused by AI systems. Finally, the question arises of (5) the geographical scope of any EU regulation.

i Fairness, bias and discrimination

One of the aims of the AI Act Proposal is to avoid risks of AI systems leading to unfair, biased and discriminated results, in particular in critical areas such as education and training, employment, important services, law enforcement and the judiciary. These are considered to have the potential of significant impact on democracy, rule of law, individual freedoms as well as the right to an effective remedy and to a fair trial.[57]

To limit these risks of erroneous or biased decisions by AI systems, providers of high-risk AI systems must implement a quality management system ensuring compliance with the obligations imposed by the AI Act Proposal.[58] This quality management system comprises an *ex ante* testing, risk-based approach and human oversight. On *ex ante* testing, prior to be put on market, high-risk AI systems must go through a conformity assessment carried out as a general rule by the third party provider.[59] High-risk AI systems must be designed in such a way that human oversight must be possible.[60]

ii Transparency and accountability

The AI Act Proposal imposes transparency obligations on high-risk AI systems to address potential risks of manipulation of users.

High-risk AI systems must be designed and developed to ensure sufficient transparency to enable users to interpret and use the system's output.[61] The information to be provided to the users includes, first, the identity and the contact details of the provider. Second, users should be informed about the characteristics, capabilities and limitations of performance of the high-risk AI system they use, including its intended purpose and its level of accuracy. Additionally, users should be informed of changes made to the high-risk AI system following an initial conformity assessment and of the human oversight measures in place. Last, users should be provided with information about the expected lifetime of the high-risk AI system and any necessary measures to ensure its proper functioning, including as regards software updates.[62]

Additional obligations will apply to a few categories of AI systems that are considered as requiring further transparency, given their sensitivity. For instance, AI systems that interact with human beings must be designed and developed in such a way that natural persons are informed that they are interacting with an AI system.[63] Natural persons using AI systems that detect emotions or determine association with (social) categories based on biometric data must be informed of the operation of the system the natural persons are exposed to.[64] Finally, AI systems that generate or manipulate image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful (also known as deepfakes) will also be required to disclose that their content has been artificially generated or manipulated.[65]

iii Intellectual property

The AI Act Proposal does not explicitly refer to intellectual property and does not deal with the allocation of intellectual property rights for content generated by AI; however, the intellectual property rights of the developers of AI systems were taken into account in drafting the AI Act Proposal.[66] For this reason, to avoid the risk that transparency obligations imposed on AI system providers could amount to infringement of their intellectual property rights, disclosure of information was strictly limited to the minimum required pursuant to the Act.[67] In addition, authorities are bound by confidentiality obligations with respect to information received under the AI Act.[68]

iv Liability

The AI Act Proposal does not cover liability of AI systems. Nonetheless, two other proposals have been put forward by the EC to regulate this area.

The first proposal, for an AI Liability Directive, aims to adapt private law to the digital economy by making it easier to bring claims for harm caused by AI systems. The Directive will provide common rules for a fault-based liability regime when damage is intentionally or negligently caused as a result of the use of AI systems (i.e., it does not address the situation where there is a damage but neither the provider nor user is at fault).[69]

The AI Liability Directive will also provide for a rebuttable presumption of causation for high-risk AI systems and non-high-risk AI systems where (1) there is a breach of duty of care by the AI system user, (2) it is reasonably likely that the fault has influenced the output of the AI system (or its failure to produce any output), and (3) the claimant proves that the AI system's act or omission has given rise to damage.[70] In addition, it establishes a rebuttable presumption of breach of duty of care for high-risk AI systems if they fail to comply with their obligation to disclose potential evidence.[71]

At this stage, the AI Liability Directive does not address situations in which an AI system causes damage but there is no obvious defective product or fault by either the provider or the user; however, the EC will assess the need for no-fault strict liability rules five years after the entry into force of the AI Liability Directive.[72]

The second proposal put forward by the EC is a Revised Product Liability Directive that expands the scope of the strict liability regime for consumers who suffer certain types of harm from a defective product to include harm caused by software and AI systems. This Directive expands the notion of harm for which a claimant can obtain compensation to include medically recognised psychological harm and the loss or corruption of electronic data (where it is not used exclusively for professional purposes).[73] Under this Directive, liability would continue to apply when a defect comes into being after a product has already been placed on the market or put into service.[74] This entails software updates under the manufacturer's control, failure to address cybersecurity vulnerabilities and machine learning.[75]

The Revised Product Liability Directive will further ease the burden of proof for claimants by establishing a presumption of defectiveness and causal link under certain conditions. Defectiveness will be presumed when (1) a manufacturer fails to comply with the obligation to disclose information, (2) a product does not comply with mandatory safety requirements or (3) the damage is caused by an obvious product malfunction.[76] The Directive will presume a casual link between the AI system and the damage when (1) the damage is typically consistent with the defect in question or (2) there is technical or scientific complexity causing excessive difficulty in proving liability (e.g., black box AI systems).[77]

At the time of writing, the EP and the Council have not yet reached an internal agreement on their negotiating positions on the EC proposals. Once these positions have been agreed, the three EU legislative institutions (the EC, the EP and the Council) will enter into trilogue negotiations to agree on the final texts. Given the end of the current EU legislature in October 2024, it is uncertain whether these texts will see the light in this cycle or will have to wait to be picked up by the newly elected EP in 2025.

v Jurisdiction

As stated above, the AI Act Proposal applies to (1) AI system providers that place AI systems on the market or into service in the EU irrespective of the place of establishment of the providers, (2) users of AI systems located in the EU, and (3) AI system providers and users located in a third country, where the output of the AI system is used in the EU.[78] The Proposal clarifies that its rules should apply to providers of AI systems, irrespective of whether they are established within the EU or in a third country.[79]

This broad geographical scope, which exceeds the territory of the EU itself, is in line with other EU rules that aim to protect final consumers, such as the GDPR.[80] Similarly, in 2022,[81] the CJEU clarified that the territorial scope of the Air Passenger Regulation[82] includes connecting flights departing from the EU and arriving in a non-EU country with a layover in the non-EU country, for a delay caused on the second leg of the flight, and that this is necessary to give effect to the legislative intent of a high level of EU consumer protection.

Enforcement

i Public enforcement

The AI Act has not yet entered into force and, therefore, has not been enforced by any public regulator. Nevertheless, as stated above, the EC has already started working on the development of a temporary and voluntary code of conduct to be agreed with European and non-European technology companies that are developing AI. After the adoption of the AI Act by the EU co-legislators, it can be expected that authorities will start engaging with companies ahead of the Act's entry into force. To date, there have been no examples of public enforcement (of other AI or non-AI legislation) against AI system providers at EU level in any field, including in the antitrust field.

ii Private litigation

Any private litigation deriving from an EU act would have to be brought at national level (i.e., in front of the courts of one of the 27 Member States). To date, however, in the absence of any AI-specific EU rules, there are still no examples of any such private enforcement.

Legal practice implications

At EU level, AI may affect legal practice for in-house use and AI detection and enforcement tools by authorities. In-house use of AI tools will facilitate monitoring to ensure compliance with EU law by companies whereas authorities may develop AI detection and enforcement tools. For instance, the EC could develop AI software to detect price agreement or suspicious bidding patterns in public procurement, or merger screening tools to detect deals that would not be notified to the EC.

Outlook and conclusions

Companies developing and offering AI systems in the EU should expect a steep increase in scrutiny from regulators in the near future, as various industry-specific legislative initiatives (AI Act, AI Liability Directive, Revised Product Liability Directive) will become applicable to their business. Even though compliance with the AI Act will be challenging, in particular for companies that are active in multiple jurisdictions and hence needing to comply with potentially diverging sets of rules, AI companies should pay attention to the EU given the potentially significant fines. Furthermore, as the obligations of the AI Act will be burdensome, in particular in relation to high-risk AI systems, early engagement with regulators is highly recommended to understand compliance with those obligations in practice before they are in force.

Endnotes

[1] Elisabetta Righini is a partner and Daphné Van der Eycken is an associate at Latham & Watkins LLP. The authors would like to acknowledge the kind assistance of their colleague Etienne Fumagalli with the preparation of this chapter. ^ Back to section

[2] European Commission (EC), 'Communication from the Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions – Artificial Intelligence for Europe', COM (2018) 237 final, 25 April 2018. ^ Back to section

[3] EC, 'Remarks of President von der Leyen at the Bletchley Park AI Safety Summit – AI safety priorities for 2024 and beyond', SPEECH (2023) 5502, 2 November 2023. ^ Back to section

[4] The European Investment Bank (EIB) reported an annual shortfall of up to €8 billion in investments to keep the EU in the global AI race. EIB, 'Main Report on Artificial intelligence, blockchain and the future of Europe – How disruptive technologies create opportunities for a green and digital economy', 1 June 2021, p. 60. ^ Back to section

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016 (GDPR), p. 1. ^ Back to section

[6] Bradford, Anu (2012), 'The Brussels Effect',*Northwestern University Law Review-*, Columbia Law and Economics Working Paper No. 533 107 (1). ^ Back to section

7 EC, 'White Paper on Artificial Intelligence – A European approach to excellence and trust', COM (2020) 65 final, 19 February 2020. ^ Back to section

8 EC, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts', COM (2021) 206 final, 21 April 2021 (AI Act Proposal). ^ Back to section

9 EC, 'Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)', COM (2022) 496 final, 28 September 2022 (AI Liability Directive Proposal). ^ Back to section

10 EC, 'Proposal for a Directive of the European Parliament and of the Council on liability for defective products', COM (2022) 495 final (Revised Product Liability Directive Proposal), 28 September 2022. ^ Back to section

11 European Parliament, 'Briefing on Digital sovereignty for Europe – Towards a more resilient EU', 1 July 2020. ^ Back to section

12 Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative act - General Approach', 25 November 2022 (Council General Approach), available at https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf. ^ Back to section

13 Garante per la protezione dei dati personali (GPDP), press release, 'Artificial intelligence: stop to ChatGPT by the Italian SA – Personal data is collected unlawfully, no age verification system is in place for children', 31 March 2023, available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847#english. ^ Back to section

14 GPDP, press release, 'ChatGPT: OpenAI reinstates service in Italy with enhanced transparency and rights for European users and non-users', 28 April 2023, available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9881490#english. ^ Back to section

15 Parliament's Negotiating Position, 'Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)', 14 June 2023, available at https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html. ^ Back to section

16 Judgment of 21 June 2022,*Ligue des droits humains*, Case C-817/19, EU:C:2022:491.- ^ Back to section

17 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (PNR Directive), OJ L 119, 4 May 2016, p. 132. ^ Back to section

18 Directive (EC) 2004/82 of the Council on the obligation of carriers to communicate passenger data, OJ L 261, 6 August 2004, p. 24. ^ Back to section

19 Directive (EU) 2010/65 of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC, OJ L 283, 29 October 2010, p. 1. ^ Back to section

20 PNR Directive (op. cit. note 17), Article 6(2). ^ Back to section

21 id., Article 6, paras. (3)(b) and 6(4). ^ Back to section

22 *Ligue des droits humains* (op. cit. note 16), paras. 194–95. ^ Back to section

23 id., para. 195. ^ Back to section

24 GDPR (op. cit. note 5), Article 22. ^ Back to section

25 At the time of writing, the final text reflecting the political deal reached between the co-legislators is not yet available. This section is based on the original EC Proposal and highlights where press releases of the co-legislators report agreed-upon changes to the EC Proposal. ^ Back to section

26 AI Act Proposal (op. cit. note 8), Article 2(1). ^ Back to section

27 Council, press release, 'Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world', 9 December 2023, available at https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/. ^ Back to section

28 The agreed definition has not been shared at the time of writing, but the Council reports that the compromise agreement aligns the definition with the approach proposed by the Organisation for Economic Co-operation and Development. See Council press release, 'Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world' cited at footnote 27. ^ Back to section

[29] id., Article 5(1). The list of prohibited practices includes (1) manipulating human behaviour or circumventing free will by deploying subliminal components individuals cannot perceive, (2) exploiting or manipulating individuals to target their vulnerabilities or special circumstances, (3) contributing to government social scoring, and (4) using biometric identification in publicly accessible spaces for law enforcement purposes (subject to certain exemptions); in addition, both co-legislators report that the political agreement should add item (4) as above (biometric categorisation systems that use sensitive characteristics – e.g., political, religious, philosophical beliefs, sexual orientation, race), (5) untargeted or bulk scraping of facial images from the internet or closed-circuit television footage to create facial recognition databases, and (6) emotion recognition in the workplace and educational institutions. Based on the Council reports, the list would also include (7) certain predictive policing practices. See EP, press release, 'Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI', 9 December 2023, available at https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai; and the Council press release cited at footnote 27. ^ Back to section

[30] id., Article 6. The full and final list of high-risk AI systems and use cases is not yet available, but it seems that the list remains wide-reaching with certain added filtering conditions intended to capture only those AI systems that present significant risks to individuals and fundamental rights. ^ Back to section

[31] id., Article 52. ^ Back to section

[32] id., Article 52. ^ Back to section

[33] id., Article 9. ^ Back to section

[34] id., Articles 10 to 13. ^ Back to section

[35] id., Article 14. ^ Back to section

[36] id., Article 15. ^ Back to section

[37] id., Article 17. ^ Back to section

[38] id., Articles 18 to 19. ^ Back to section

[39] id., Article 21. ^ Back to section

[40] ibid. ^ Back to section

[41] id., Article 61. ^ Back to section

[42] id., Article 26. ^ Back to section

43 id., Article 27. ^ Back to section

44 id., Article 71(3). ^ Back to section

45 id., Article 71(4). ^ Back to section

46 id., Article 71(5). ^ Back to section

47 id., Article 65(2). ^ Back to section

48 id., Article 65, paras. (2), (5) and (9) and Article 66(2). ^ Back to section

49 id., Articles 56 to 57. ^ Back to section

50 id., Article 58. ^ Back to section

51 id., Article 59, paras. (1) and (2). ^ Back to section

52 Parliament's Negotiating Position (op. cit. note 15). ^ Back to section

53 Council General Approach (op. cit. note 12). ^ Back to section

54 Foo Yun Chee, 'EU, Google to develop voluntary AI pact ahead of new AI rules, EU's Breton says', Reuters (24 May 2023), available at https://www.reuters.com/technology/eu-google-develop-voluntary-ai-pact-ahead-new-ai-rules-eus-breton-says-2023-05-24/. ^ Back to section

55 Reuters, press article, 'EU's AI Act could exclude open-source models from regulation', 7 December 2023, available at https://www.reuters.com/technology/eus-ai-act-could-exclude-open-source-models-regulation-2023-12-07/. ^ Back to section

56 EC, 'The Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems' 30 October 2023, available at: https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-international-code-conduct-advanced-ai-systems. ^ Back to section

57 AI Act Proposal (op. cit. note 8), Recitals 15 and 40. ^ Back to section

58 id., Article 17. ^ Back to section

59 id., Article 19. ^ Back to section

60 id., Article 14. ^ Back to section

61 id., Article 13(1). ^ Back to section

[62] id., Article 13(3). ^ Back to section

[63] id., Article 52(1). ^ Back to section

[64] id., Article 52(2). ^ Back to section

[65] id., Article 52(3). ^ Back to section

[66] Based on the press releases of the co-legislators, it seems that the final text will explicitly align with the EU legal framework on copyright by allowing right holders to opt out of text and data mining for commercial purposes. ^ Back to section

[67] EC, 'Explanatory Memorandum of the AI Act Proposal', COM (2021) 206 final, 21 April 2021, p. 11. ^ Back to section

[68] AI Act Proposal (op. cit. note 8), Article 70. ^ Back to section

[69] AI Liability Directive Proposal (op. cit. note 9), Recitals 7 and 9. ^ Back to section

[70] id., Article 4. ^ Back to section

[71] id., Article 3. ^ Back to section

[72] id., Article 5. ^ Back to section

[73] Revised Product Liability Directive Proposal (op. cit. note 10), Article 4. ^ Back to section

[74] id., Article 6. ^ Back to section

[75] ibid. ^ Back to section

[76] id., Article 9. ^ Back to section

[77] ibid. ^ Back to section

[78] AI Act Proposal (op. cit. note 8), Article 2(1). ^ Back to section

[79] id., Article 2(1)(c). ^ Back to section

[80] GDPR (op. cit. note 5). ^ Back to section

[81] Judgment of 7 April 2022,*United Airlines*, Case C-561/20, EU:C:2022:266. ^ Back to section

82 Regulation (EC) No. 261/2004 of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealing Regulation (EEC) No. 295/91, OJ L 46, 17 February 2004, p. 1. ^ Back to section

LATHAM & WATKINS LLP

Elisabetta Righini elisabetta.righini@lw.com
Daphné Van der Eycken daphne.vandereycken@lw.com

Latham & Watkins LLP

Read more from this firm on Lexology