NEW YORK UNIVERSITY
JOURNAL OF LAW & BUSINESS

VOLUME 20 SUMMER 2024 NUMBER 3

THE FRONTIERS OF ARTIFICIAL INTELLIGENCE REGULATION: FIVE PERSPECTIVES FROM THE EUROPEAN UNION

ANDREW G. LIN*

Eight years after the European Union adopted the General Data Protection Act (GDPR),[1] it passed additional legislation designed to address the meteoric and transformative rise of artificial intelligence. On March 13, 2024, the European Parliament adopted the Artificial Intelligence Act ("AI Act").[2] The AI Act seeks "to protect fundamental rights, democracy, the rule of law and environmental sustainability from high-risk AI," as well as to encourage innovation and establish Europe as a leader in AI technology.[3]

The AI Act followed a flurry of legislations enacted by the European Union in the last decade. These legislations include the GDPR, the Data Act, Data Governance Act, the Digital Markets Act. Together, these legislations regulate the collection, retention, and use of data involving the E.U. or E.U. subjects.

[*] Editor-in-Chief, *Journal of Law & Business*, 2023-2024; J.D., New York University School of Law, 2024; B.S., Duke University, 2019.

[1] Press Release, Eur. Parliament, Data Protection Reform—Parliament Approves New Rules Fit for the Digital Era (Apr. 14, 2016), https://www.europarl.eropa.eu/news/en/press-room/20160407IPR21776/data-protection-reform-parliament-approves-new-rules-fit-for-the-digital-era?quizBaseUrl=https%3A%2F%2Fquizweb. europarl.europa.eu.

[2] Press Release, Eur. Parl., Artificial Intelligence Act: MEPs Adopt Landmark Law (Mar. 13, 2024), https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law.

[3] *Id.*

The AI Act entered into force on August 1, 2024 and will become generally applicable by August 2, 2026.[4] Its scope is sweeping. Not only does the AI Act impart detailed obligations on data providers and end users regarding permissible uses of artificial intelligence and machine learning models, but it also imposes extraordinarily heavy fines.[5] How private actors navigate the AI Act, and how Brussels responds in turn, will be of paramount importance to Washington and London as they continue to craft their own national artificial intelligence and data protection legislation. Indeed, all eyes are on Europe.

In recognition of the importance, complexity, and timeliness of artificial intelligence legislation, The *Journal of Law & Business* interviewed five leading E.U. policymakers and practitioners to gather their thoughts on the AI Act and related legislation.

Peter Ide-Kostic, a veteran E.U. policymaker of more than two decades, begins the conversation. He served as an Administrator in the AI in the Digital Age (AIDA) special committee, the organ that crafted the AI Act. In his remarks, Mr. Ide-Kostic reveals the political process by which the AIDA committee came about, including the selection of the committee members and the concerns of the committee during the drafting process. By illuminating the politics that brought about the AI Act, Mr. Ide-Kostic provides us with important context for making sense of this sweeping legislation.

Dragos Tudorache, chair of the AIDA committee and one of the two chief negotiators of the AI Act, continues the conversation by detailing the negotiations process with different industry stakeholders. In his remarks, Mr. Tudorache discusses several important points, including (1) the adoption of the risk-based analytical approach, (2) the delivery of standards (and the decision to depart from the approach taken in the GDPR), and (3) the imposition of obligations on data providers and end users. Mr. Tudorache also previews the implementation and enforcement process scheduled to occur over the next two

[4] Press Release, Eur. Comm'n, European Artificial Intelligence Act Comes Into Force (Aug. 1, 2024), https://europa.eu/newsroom/ecpc-failover/pdf/ip-24-4123_e n.pdf.

[5] Art. 99: Penalties, Ch. XII, EU Artificial Intelligence Act ("Non-compliance with the prohibition of the AI practices referred to in Article 5 shall be subject to administrative fines of up to 35 000 000 EUR or, if the offender is an undertaking, up to 7 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.").

years, as well as the E.U.'s coordination with legislative efforts by American policymakers.

Jérôme Phillipe, of Freshfields, shifts the conversation from the perspective of a policymaker to a seasoned practitioner. Mr. Phillipe believes that the AI Act, while extremely structured, is too cumbersome and, in many ways, premature. In his remarks, Mr. Phillipe notes that industry clients face significant uncertainties with respect to the AI Act's risk-based approach. He posits that in all likelihood, no one would be able to fully comply with the extensive requirements set forth by the AI Act. In addition, Mr. Phillipe comments on the regulatory hurdles faced by companies and points out the wide-reaching implications of the AI Act, particularly its impact on an entity's commercial policy.

Nick Wolfe, of Skadden, predicts that the AI Act will usher in a new wave of antitrust enforcement actions. In his remarks, Mr. Wolfe traces the evolution of EU and UK enforcement efforts from 2000 to the eve of the AI Act, providing the historical foundation from which the AI Act emerged. In addition, he attributes the rise of generative AI as a driver of technological uncertainty, positing that it is one of the main reasons why regulators are requesting companies for more information on transactions.

Lauren Cuyvers and Toni Pitesa, of Sidley Austin, focus on the relationship between technology, regulation, and innovation. As a threshold matter, they acknowledge the reality that AI regulation will almost always be behind the technology. In their remarks, they examine the regulatory challenges around maintaining the datasets necessary to train artificial intelligence models. They also examine the AI Act's potential anticompetitive effects due to the burden of compliance placed on startups. They acknowledge the difficulties of proactively addressing regulatory challenges posed by novel technologies, and advocate for reliance on traditional legal frameworks as a north light for *ex ante* guidance.

The five interviews offer a broad spectrum of perspectives on the AI Act from a diverse group of individuals. As the *Journal* celebrates our 20th anniversary this year, we are fortunate to have these leading policymakers and practitioners share their insights into the AI Act. Their remarks deliver valuable guidance on how businesses—from the largest companies to the earliest startups—should think about and navigate the regulatory uncertainty surrounding artificial intelligence in the twenty-first century.

NEW YORK UNIVERSITY
JOURNAL OF LAW & BUSINESS

VOLUME 20 SUMMER 2024 NUMBER 3

DEVELOPING THE EU ARTIFICIAL INTELLIGENCE ACT

PETER IDE-KOSTIC*

A. THE BIRTH OF THE AI ACT

In response to the urgency underscored by the President of the European Commission, Ms. Ursula von der Leyen, who committed to prioritizing AI legislation within her first 100 days after her appointment following the EU elections in May 2019, the European Parliament began actively preparing for future AI legislation to be introduced by the European Commission. This initiative aligned with the European Commission's publication of the "White Paper on Artificial Intelligence: A European approach to excellence and trust" on February 19, 2020.

To facilitate this, the European Parliament formed the Special Committee on Artificial Intelligence in a Digital Age (AIDA), which started its work in September 2020. The committee's activities, centered on conducting parliamentary

[*] Peter Ide-Kostic is an Administrator in the European Union Parliament's Office of the Secretariat for the Internal Market and Consumer Protection Committee. Prior to rejoining the Office of the Secretariat, he was a visiting scholar at the Center for Commerce and Diplomacy at the University of California San Diego, where he focused on AI law-making in a complex global context. Peter's extensive work both on various Artificial Intelligence Committees including the Special Committee for Artificial Intelligence in a Digital Age has provided him ample opportunity to study observe and support the regulatory process as it related to Artificial Intelligence. Peter also worked in 2019 and 2020 for the Secretariat of the Civil Liberties, Justice and Home Affairs Committee of the European Parliament and covered their AI works during that period as well. Disclaimer: The views expressed are his own and do not represent the European Parliament or other EU institutions.

research, facilitating expert hearings, and engaging with various stakeholders, culminated in delivering a comprehensive report in December 2021, adopted in the Plenary session of the European Parliament in March 2022.

Concurrently, the European Commission launched a public consultation phase from February 19, 2020, to June 14, 2020. The insights gathered during this period informed the drafting of the AI Act, which the Commission published in April 2021. However, legislative work by the European Parliament did not commence at that time, as the AIDA Committee's efforts were still ongoing.

By the end of 2021, the groundwork laid by the AIDA Committee had significantly advanced, effectively supporting the legislative process on the AI Act. This progress led to the appointment of two co-rapporteurs on the AI Act in early 2022: Mr. Dragoș Tudorache (Renew political group, Romania) for the Civil Liberties, Justice, and Home Affairs (LIBE) Committee, and Mr. Brando Benifei (Political group S&D, Italy) for the Internal Market and Consumer Protection (IMCO) Committee.

On 11 May 2023, following the introduction of thousands of amendments by the seven political groups of the European Parliament, the IMCO and LIBE Committees co-adopted the proposal to amend the draft AI Act. The European Parliament then adopted the report one month later on 14 June 2023 during its plenary session.

Given the wide scope of the AI Act, balancing the core interests of both industry and fundamental rights protectors presented significant challenges, often due to conflicting priorities. Recognizing the importance of balanced representation, the political groups selected members with diverse political backgrounds but with significant experience from their work in the AIDA Committee. This strategic selection included Mr. Tudorache from the center-right Renew group for the LIBE Committee, which is competent on fundamental rights (a topic more often associated with the left), and Mr. Benifei from the left-center Socialist group for the IMCO Committee, which concentrates on market development, consumer protection, and innovation (topics more often associated with the right). Their combined experiences and political sensibilities ensured a legislative proposal that was amenable to all stakeholders involved.

Additionally, other Committees such as Legal Affairs (JURI), Culture and Education (CULT), and Industry, Research, and Energy (ITRE) were also involved in the legislative process of amending the AI Act, though their participation was limited to areas within their specific competencies.

B. Shifting the Paradigm: The Rise of General-Purpose Artificial Intelligence Models

Up to November 2022, the European Parliament focused on the concept of AI systems operating within the common market. However, AI models and their training methods remained unregulated. The introduction of ChatGPT and the rise of foundation models—a term initially coined by Stanford and later rebranded as General-Purpose AI models—highlighted a significant oversight. These developments indicated that legislation limited to AI systems could not adequately protect fundamental rights or sustain healthy innovation and competition.

It is noteworthy that neither the European Commission's draft AI Act from April 2021 nor the European Parliament's AIDA report from March 2022 addressed General Purpose AI models. The need to regulate them became evident during the legislative amendments of the AI Act made by the European Parliament between January 2022 and May 2023.

The widespread impact of ChatGPT in November 2022 is, in fact, the main factor that underscored the need to regulate highly capable General-Purpose AI models due to their potential systemic risks for the EU internal market.

This realization is the main reason that led to an extension of the legislative process in the European Parliament, with the amended AI Act not being finalized until June 2023.

C. Trilogue to Adoption

The added complexity and additional policy challenges posed by the legislation of General-Purpose AI models (GPAIs) are key factors that complicated the final phase of the EU legislative process, along with the provisions related to law enforcement and national security.

During the final phase of the legislative process, a procedure known as "Trilogue" took place between July 2023 and December 2023. During this period, the European Parliament and the European Council confronted their respective amended versions of the AI Act. With the support of the European Commission, which initially drafted the text in April 2021, the two institutions reached the final compromised version of the text that is expected to become law in mid-2024 at the time of writing this article.[1]

The wide range of stakeholders involved made negotiations often extremely difficult. The negotiations were led by the two co-rapporteurs, Mr. Tudorache and Mr. Benifei, from the European Parliament side, and on the Council side by Ms. Carme Artigas of the Spanish government, which held the rotating presidency of the EU Council until the end of 2023. These negotiations culminated over an almost uninterrupted three-day period on December 6, 7, and 8, ending with clear political agreements on all sensitive areas of the text.

Convincing large western EU member states fell to the EU Council, primarily represented by Carme Artigas of Spain. Her efforts to bring France and Germany to the table were instrumental in reaching a final agreement. Another concern was industry stakeholders, particularly small and medium enterprises (SMEs) and AI startups that contributed to the release of free open-source AI models (such as Mistral and AlphaDev in the EU). There were fears that over-regulation could disadvantage smaller companies vis-à-vis larger ones, as well as EU companies compared to US counterparts in some markets.

Concerns about IP protection and competition were also raised, alongside the protection of core fundamental rights. The final 36 hours of these negotiations were extremely difficult, but late on the night of December 8th, an agreement between the three bodies was reached on all sensitive areas of the legislation.

On February 13, 2024, the LIBE and IMCO committees approved the text of the act, followed by the Parliament adopting the act on March 13th. The lengthy task of reconciling the final language in the document then began. The nature of the EU means this is a particularly long task involving lawyer-linguists in all official languages of the EU and all Member States. Differences in language, compounded by differences in context and meaning, complicate translations and sometimes result in the need to consult at the political level to ensure that the translated text correctly reflects the intent of the legislator in all languages.

[1] This version of text became applicable law on 1 August 2024.

Linguistic agreement from all member states was reached during March 2024 and formally endorsed on 18 April 2024 by the European Parliament.

At the time of writing this article, the text is expected to be endorsed by the European Council during May 2024 and to become law in June 2024. Twenty days after publication in the Official Journal of the EU, the AI Act will come into effect, and implementation will begin.[2]

[2] The European Council adopted the text on 14 June 2024, shortly after the European elections held from 6-9 June 2024, and it was published in the Official Journal of the European Union on 12 July 2024. Finally, the AI Act came into effect on 1 August 2024, with its implementation beginning immediately thereafter.

NEW YORK UNIVERSITY
JOURNAL OF LAW & BUSINESS

VOLUME 20 SUMMER 2024 NUMBER 3

INSIGHTS FROM THE DELIBERATION ROOM: NEGOTIATING THE EU'S AI ACT

DRAGOȘ TUDORACHE*

SCOTT PATTERSON:

Thank you for joining us today Mr. Tudorache to discuss the EU's AI Act. Diving right in, can you speak to the negotiations between the committees involved in crafting the AI act? Specifically, the points of emphasis for each party, sticking points, and common themes of agreement.

DRAGOȘ TUDORACHE:

I think what was one of the many things that was special about this AI Act, because there were many things that were somewhat out of the ordinary even for European Standards, was that we've had a record number of committees that were part of this set up at Parliament level. So traditionally you have one committee that's responsible for negotiation with one lead negotiator, one lead rapporteur, for one legislative file; while in this case we had two leading committees. The one on civil

[*] Dragoș Tudorache is a Member of the European Parliament and Vice-President of the Renew Europe Group. He is the LIBE rapporteur on the AI Act, and he sits on the Committee on Foreign Affairs (AFER), the Committee on Civil Liberties, Justice and Home Affairs (LIBE), the Committee of Inquiry to investigate the use of Pegasus equivalent surveillance spyware (PEGA), the Subcommittee on Security and Defense (SEDE), and the European Parliament's Delegation for relations with the United States (D-US). He was the Chair of the Special Committee on Artificial Intelligence in the Digital Age (AIDA). Disclaimer: The views expressed are his own and do not represent the European Commission or other EU institutions.

liberties[1] and the one on the internal market[2], and plus a plethora of other committees that had bits and pieces of competence for different parts of the text which of course made the preparation and negotiations both inside of Parliament and then with the council even more difficult, more complex, because then inside each of these committees you have all of the political groups, each of them carrying the flavor of that respective committee and the priorities of that respective committee. And that made for a very complex multi-layered negotiation and that's why it also took a bit longer than usual. In terms of sticking points, it is difficult to categorize which were more problematic than others but very quickly we have zeroed in on definitions, which from the beginning we wanted to get right, understanding how important they will be for putting the right framework around what we wanted to be part of the scope of the regulation and what we did not want to make part of the regulation. Then also, with the ambition to keep these definitions as aligned as possible with what was happening in other fora and with other jurisdictions out there, we aimed to align with the definitions of the OECD, and the definitions also on the US side. We also discussed with the National Institute for Science and Technology (NIST) as we wanted to make sure that these definitions will be aligned as much as possible to help for the global conversation, the global convergence that we knew we would need to strive to achieve.

Then there was a very long and complex discussion on how to define the governance around high risks. We knew that we would have a list of contexts of AI applications that we would be labeling as high risk, but how exactly to calibrate the norms, whether it would be for all applications that would be developed in that particular context, or if only for part of them, how do you define the thresholds for those that would be entering the scope and those that would be outside the scope? And eventually we ended up with a number of criteria to determine what represents a significant risk and therefore can see as the need for conformity. Additionally, we had very long and complicated negotiations on some of the prohibited applications, particularly on the use of biometrics in public spaces in real time, where

[1] The European Parliament's Committee on Civil Liberties, Justice, and Home Affairs, colloquially known as the "LIBE" Committee.

[2] The European Parliament's Committee on the Internal Market and Consumer Protection, colloquially known as the IMCO Committee.

there was a part of the House that wanted from the very beginning an outright ban on the use, employment of this technology, and others who were seeing a need to create an exception for law enforcement and access by law enforcement, to some of this technology in order to ensure an efficient, effective fight against particularly very serious criminality. That remained one of the sticking points all the way until the very end, even in the negotiations between parliament and council.

Then of course, the big discussion on foundation models. The discussion that came in later in the negotiations, there we spent quite a lot of time.

I can go on and on and on, almost all of it was a difficult negotiation in itself, but these were some of the highlights.

Scott Patterson:

One follow on question: did you all settle on the risk framework and determine what was high risk prior to foundational models and general-purpose AI models coming out, or was that a post ChatGPT discussion?

Dragoș Tudorache:

Well, when we started our work, the proposal was a risk-based approach identifying the applications, the areas in which applications of AI would be raising risk. And there was an annex which listed those areas such as recruitment, education, health, banking, insurance, and it's important to note that this started before ChatGPT.

But already in the course of all preparations we were starting to play with what we called back then general-purpose AI, recognizing that it represents a challenge in sticking to the logic of the risk-based approach, with applications that in themselves did not represent a risk or were not allocated a purpose that represented a risk in itself. Because they were, for example, language processors. On the face of it, what's wrong or can be risky about a language processor? But then we realized that by the very nature of how these models are developed, the way they are trained, their versatility, their potency, we realized there is something about them that actually can have quite a significant impact, both in the value chain for other systems that will be developed on top of these models, but also for the customers, for the clients, for the individuals rights themselves. So therefore, we started with a discussion as to whether these models should be put in the category of high risk or not.

We then agreed that putting them in the category of high risk would not actually do justice to them and we also would be affecting the mechanism that we were just preparing for the high-risk applications. That is how and when we decided to craft a special regime for foundational models. This was already autumn of 2022, just maybe a month or so before November when ChatGPT was launched. We had already decided by then that we wanted to deal with foundation models in our text and that we wanted to have a special regime for it. And what we set out to do was to identify what would be the obligations that we considered would be specific for these models.

When ChatGPT came, in a way it proved that it was worth considering a special regime for these models because we could very quickly see how important and how impactful they will be. It also allowed us to then filter through all of the information, and also now having the actual technology in our hands, it was easier, it helped us define exactly how we want to regulate it, what kind of rules we want to put in place. And by Spring 2023, we were able to have this regime fully down, mandate, negotiate, and approve it.

We recognized already that we might need to further work on the text as we would start the negotiation with the council. Our counterpart, the other co-legislator, had nothing in their mandate related to that so we knew that there would be a lot of discussion there, and it proved to be the case. It was one of the open issues up until the very last night of negotiations in December of last year. But that was the journey away from having nothing in the text about foundation models to the point where we are today.

Scott Patterson:

Thank you. Touching on what you spoke briefly about collaborating with NIST and making sure that you were somewhat aligned with what they were also looking at, can you speak a little bit more to the concerns of US stakeholders and what concerns they brought to the table during the negotiations? Both companies and regulatory-wise.

Dragoș Tudorache:

Companies have brought a lot of arguments to the table, and I can't even filter out which were American companies and which were European companies. I never, in fact, categorized them that way. My policy has been one of an open door towards anyone, any stakeholder that had contributions to make, an argument to bring, because I considered that to be an education for me as a lawmaker, I want to make sure that I hear all possible positions and arguments and learn from them. And I treated companies in the same way – I didn't treat them as lobbyists, I treated them as contributors to the debate.

One of the main arguments coming from some of the bigger players on the US side was that foundation models did not need regulation at all because they were not designed with a particular purpose in mind, a purpose that would be prone to risks, and therefore the responsibility was not theirs. And that the responsibility should be further down the value chain with entities that would be taking their models and developing applications on top that would then raise risks or come in one of the risk categories; and therefore if we were to regulate somehow, we had to regulate the downstream and not the upstream. That was one argument that they brought forward.

Then another argument that they brought was that it was irrelevant and not necessary to require transparency of the data sets used to train the algorithms because well first of all they said it's not necessary, then they moved the cursor and said that would be a problem of trade secrets, and it's part of the recipe of the model and therefore forcing them to be transparent about that would be forcing them to release trade secrets. So, they've used all sorts of arguments to mainly escape altogether responsibility. And then once they realized that that would not happen, that there would be nevertheless a set of obligations, a regime that would be applicable to them, then the discussion moved into trying to make that as flexible as possible with an argument, I think a very good argument and one that we eventually used in our discussions, which is that the technology was still nascent, there was still a lot that we did not know, it was also very fluid, changing all the time.

This is why we chose a model where we listed the obligations in the text to make it clear what we expect out of the developers of these models, but at the same time we recognize that there are no set tools, technologies, or standards yet for how you comply with those obligations. And that is why we accepted the logic of working with a code of practices at the beginning. This is a form of flexible enforcement in the first phase, where the enforcer at the EU level would be interacting with these developers to see how best they can respect the obligations that they have in terms of risk management, in terms of incident reporting, and in terms of transparency.

Once this Code of Practice is co-designed, then it is going to be fixed in law by virtue of secondary legislation that will be adopted by the European Commission together with the future AI office, until, and this is a placeholder, until standards will be available. So, I think that we've listened and accepted those arguments related to flexibility. And I think we did right, we did justice to where the technology is today. And to the need for working together, for co-generating the standards and the methodologies that will be used to respect these obligations.

And then in terms of the interaction with the US administration, at the level of the European Commission, between the administrations themselves, there was quite a lot of contact and cooperation as part of the TTC framework. But as legislators, we also made sure that we paid attention to what was happening on the US side, also making sure we are informing fellow lawmakers in Congress as to the evolution in our negotiations. I think that helped a lot also in the way the White House has eventually prepared the executive order, and in fact if one unpacks the executive order, there's quite a lot of approaches which are similar, and some of the effects of the executive order would not be very different even if it takes a sectoral approach. So, I think that this coordination, this cooperation, worked well for both sides.

Scott Patterson:

Thank you for that. Shifting gears to the regulatory framework and the actual implementation and enforcement. How do you envision the AI office working with both companies and Member States to ensure that compliance is met and ensure that the Legislative Act is being followed?

Dragoş Tudorache:

The big challenge, in fact, starts now. Yes, it was very complicated to get to today, to actually have the AI Act in place. But now implementing it is going to be even more difficult.

So, first and foremost, the office will have to get itself ready, and it will have one year to do so. Because in one year's time it will start applying this regime for foundation models, for which the office has exclusive competence.

That means that by that time, the office will have to have the right people in place. The right methodologies for testing, for evaluations, and for red teaming. So quite a tall order for the office in the next one year, to be ready to take on the likes of ChatGPT, Gemini, Claude, and all the applications that will be making it past the threshold that we have established. And, by the way, another obligation for the office is to always be on the lookout for the evolution of the technology, constantly consult with the scientific community to make sure that those criteria that are supposed to be used for differentiating within models, those are flexible. And they are deliberately flexible in the regulation, understanding that the criteria that we use right now – the FLOPs – might be totally irrelevant in one year's time because in the meantime the use of infrastructure might change with these models.

So the AI office will have this responsibility to keep the regulation in a way adapted to the evolution of the technology. Then the national regulators will also kick in with their part of the competence which relates to the application of the high-risk framework for all other AI applications out there. That is, when an additional layer of complexity comes in. Coherence and uniformity in interpretation, application, will be fundamental to avoid some of the mistakes that we did with the GDPR, for example, where we ended up with quite a lot of fragmentation between the different jurisdictions in the Member States with the GDPR being understood and applied differently between Member States. And that's something we don't want with the Act; it's key that we ensure this coherence. So, this interplay between the EU level governance and the national level governance will be fundamental for good application, good implementation, good enforcement of the law.

Its difficult to predict how it will work because there is no blueprint for it. It's the first time that this sort of governance actually is put into place. A lot of learning and flexibility and adaptability, and an open mind which will have to be kept both by the national regulators and the European Regulator in order to make this work and keep the spirit of the law as we intended it, as legislators, as alive and as true to the cause as possible.

Scott Patterson:

That makes total sense and thank you for explaining. I know the implementation of the Act hasn't been released or put forth yet so getting insight on how you envision the enforcement of the regulation is pretty key moving forward, especially both for companies and for future lawyers.

Dragoş Tudorache:

One point that I forgot to say, which is also incredibly important for the application, the implementation of the law, is the delivery of the standards. This is the one thing that we did differently from the GDPR. We've given a mandate for technical standards to standard setting bodies at the European level and they have two years to deliver now until the moment when the regulation kicks in also at the national level.

The European Commission delivered a set of guidelines for different parts of the text, where we consider that further technical explanation is necessary for companies to understand how they need to do their self-assessment, how they need to interpret the threshold of significant risk, for example, in the high-risk category. So all of those clarifications will need to come in the next two years until the full entry into force of the legislation, in order to give clarity and predictability of the norm for companies. And also, very importantly, to give this clarity in a technical form not in a legal or legalistic way, which sometimes legislation tends to be, to help companies, particularly the smaller ones, that cannot afford big compliance teams or hire law firms to tell them what they need to do, to allow them to self-assess, looking at the set of technical standards and understanding what it is that they need to do.

Scott Patterson:

It makes total sense. It gives you the flexibility to move forward and adjust as you see how a regulation actually unfolds.

Is the AI office meant to be an independent, regulatory body, or will it be staffed with representatives from the Member States, or just with experts from different particular committees, such as the IMCO or the LIBE committees. How do we look at the future of the AI office staffing?

Dragoş Tudorache:

We meant it, and we mean it as an autonomous structure. We've placed it inside the European Commission in order to achieve synergies, understanding that it's not going to be easy to find the right level expertise, convince them to come and work for the public sector on salaries that are not necessarily on par with what the industry offers. And, knowing that the Commission already has teams in place to implement the DSA or the DMA, we thought it's going to be easier if we also place the AI offices at the Commission, we give it sufficient autonomy to function and to perform its very different competencies compared to the DSA and the DMA offices. But it has a dedicated structure, it has a dedicated budget line, and we insisted very much on that, and it also has the ability to recruit from inside or from outside the Commission freely, in order to attract talent as flexibly as possible.

What is happening right now is that the Commission has already transferred some staff from the current Directorate General responsible for digital issues inside the European Commission. So they are, in a way, the backbone of the office. They will ensure the policy continuity in terms of understanding what is required, particularly on the regulatory side, the further guidelines that will need to be done, the interaction with the standard setting bodies, what are the adaptations of the regulation and the further secondary legislation that will need to be ensured. Plus, they will be the ones that will be taking care of the governance once the national regulators come together in the Board, because there will also be a Board, with all of the national regulators. And then the creation of the Scientific Committee and the creation of the Advisory Group. Together they will form the governance for the AI Act.

But at the same time the office will have to have technical staff, the ones that will be developing the tools, the methodologies for evaluation and testing the ones that will be interacting on a regular basis with the companies developing the big models, so on and so forth. And for that, the office will have to look outside, because those experts do not exist in the Commission right now. They are now in the process of hiring, they have already issued vacancy notices for technical staff, and they will be on the lookout for the year ahead to try and attract as much talent as possible. Most of that, if not all of that is in the private sector, so it's going to be quite the challenge to bring them in. A challenge that from my contacts with the UK Safety Institute and the US Safety Institute, I think, will be shared across jurisdictions because it's not going to be simple to bring in that kind of talent from the private sector to a public institution. But I remain hopeful that in the next year they'll manage successfully to also bring in such staff.

Scott Patterson:

Thank you for that. Shifting gears to the final topic. We've covered the negotiations and what the interests were. We've covered where the regulatory framework is going, what the regulatory process will look like.

But now, turning to the Act itself. We know that the LIBE committee, which typically handles fundamental rights, and the IMCO committee, which typically handles the internal market and industry, were co-heads.

So, one question we had for each committee is how the core elements of the AI Act protect fundamental rights? And then how do they promote industry and innovation on the other side?

DRAGOŞ TUDORACHE:

This was from the start; our ambition to achieve the necessary protection of individual rights and societal interests, while at the same time promoting innovation and competitiveness and we constantly worked to blend the two objectives of the text so that they don't appear as a binary choice, as a zero sum game between the two, or that there is some sort of conflict between the objective to protect and the objective to stimulate innovation. I think what we achieved is a good balance between the two.

Now I'll be specific. On the protection side, the regulation was already built from the get-go on the idea of having a human centric focus of the regulation; looking at the risks that are related to individual rights or to the broader interests of society. But even there, in the negotiations, and particularly through amendments and work that was done in the European Parliament, we've added several layers of extra protections.

First of all, we've added to the list of prohibitions, a number of applications that we thought needed to be there. I'll give some examples – predictive policing, or biometric categorization – so things that we thought need to be there because it was fundamental to how we understood privacy or how we understood fundamental rights, and rule of law in the Union. The same thing when it comes to the list of high risks, for example the idea of a fundamental rights impact assessment for all deployment of high-risk applications, particularly in the in the public sector.

Why? Because, history and practice has shown that it is in the public sector where the potential for breaching is, and is the highest risk, and unfortunately, we already had practical examples in Europe. We had the famous case in the Netherlands with the social security system that was using an algorithm to determine potential fraud to the social security schemes and which was completely biased against non-natives, basically, of that particular Member State.

And then similar other cases which showed that, particularly when you apply artificial intelligence in the public sector, you need to have that extra care, and you need to have an active drive as a public institution before you actually decide to deploy such an AI tool in your public service. You have to have an extra duty of care on making sure that that application of artificial intelligence is not breaching rights. So that's why we introduced this impact assessment upon deployment in these sectors.

We've also introduced redress, individual and collective, something that was completely missed in the initial proposal of the text, because we thought that it was also fundamental that consumers and individuals have a way to bring their case before the authority, and eventually before the courts if they would find that one particular application of AI was detrimental to their rights. We chose that path because we thought that with AI becoming such a normally present technology in all walks of life, in almost every sector of human activity or economic activity, it will be quasi-impossible for the regulator to always keep an eye and make sure that they actually know everything that goes on. So, you need these bottom-up reporting mechanisms if you want an alarm system from the consumers themselves to identify potential problems with the interaction between human and machine. So that's why redress was an important mechanism, and I'm proud that it is now in the system.

Now on the innovation side from the beginning, we said, there must be enablers in this text that will be lowering the cost of compliance. So even where compliance will be necessary, we wanted to make sure that compliance does not act as a barrier for innovation or for entry to the market, particularly for smaller companies. So that's why we wanted to make the cost of compliance as low as possible. That's why we went for self-assessment. That's why we went for technical standards to make sure that if you want to go on the market with a product, and you're a startup of two or three people, and you cannot afford to pay a lawyer or a compliance team, you have your technical standards available, you can read and understand them. You do your self-assessment and you can judge for yourself whether you are in one category risk or another, and what you have to do to go on the market.

We've also completely changed the philosophy of sandboxes. The concept of sandboxes existed in the initial provision of the text, but very much like an extraordinary testing ground. Whereas we turned it into almost a pre-compliance enabler, particularly for smaller businesses, who, are still uncertain after they looked at the technical standards and have done their self-assessment, but let's say they are still not sure – am I actually a significant risk? Am I passing the threshold, or am I not? Well, then, they have the possibility to go into a sandbox; a sandbox that national authorities will be obliged under the AI Act to establish at the national level, but also at the regional and municipal level, so that companies and startups, can go, enter into a sandbox, interact with the regulator, test, validate their assumptions, validate their data sets, and prepare for compliance, achieve pre-compliance in that controlled environment where they can also make mistakes, they can say stupid things, they can check things with the regulator before, achieving certainty that when they go on the market they go in a compliant way.

Many other examples, special provisions for SMEs, special provisions for research and development, special provisions for open source. So we've looked, in a way, at the ecosystem of AI as it is today, a lot of it actually with SMEs, very agile small players, and we wanted to make sure that they will continue to feel stimulated, to remain, to grow, to develop, to innovate without fear that all of a sudden if rules come to town they will have to close shop or they will have to fundamentally change their business model. To the contrary, we gave them tools to continue to do what they do without much hinderance.

SCOTT PATTERSON:

And just to confirm, SMEs are small enterprises?

DRAGOȘ TUDORACHE:

Small and medium enterprises, yes. This is the European jargon for small companies.

SCOTT PATTERSON:

We all have our own abbreviations! A quick follow up on the redress capability that you mentioned. Would this be akin to a private right of action on the European side?

DRAGOȘ TUDORACHE:

Yes.

SCOTT PATTERSON:

Okay, I wanted to confirm that as well. That wraps up most of my questions. The next question is on speaking to law students or future legal professionals. I wanted to confirm, you were a judge previously, right?

Dragoș Tudorache:

Yes, I was. Way back.

Scott Patterson:

Okay. For any lawyers or future lawyers who are looking to either regulate or represent and advise companies, what advice would you have for them in light of where the regulation is moving, based on your experience negotiating the AI Act and shepherding it through the inception of AIDA all the way to now?

Dragoș Tudorache:

I think rules around this technology and generally rules around digital and the online realm, even if right now they seem to be mostly emanating out of the EU, I'm convinced that in the not very distant future, this will become the norm in most other jurisdictions. I think it's inevitable, to a certain extent, at least, for some parts of the online reality. It is late because some of the risks have materialized already. If we look at social media and what it has done to the cohesion of our societies, already we are intervening late by expecting certain responsibility for the platforms, and how they work, and how they optimize and so on and so forth.

So, what I'm trying to say is that I consider rules to now become inevitable for a sector that operated in a vacuum for a very long time, which means that with rules becoming a reality, lawyers will now need to also themselves prepare, adapt and learn. So, the first observation to make is that I consider that every lawyer will need to start understanding technology as well. I know that many universities already started to blend ethics of technology and how it plays out into society and economic relations, into legal studies; I think that's a good approach.

Then companies themselves, as these rules, these norms, these standards, will become more and more present in most jurisdictions, companies themselves will need to understand how they navigate these rules. So, they will be asking lawyers for help.

So, from my point of view, there's a lot of opportunity that actually is opening up right now for lawyers and for how their services will be requested in the future. There is also a question that I think lawyers need to ask themselves in terms of the impact that AI has on their own job, because lawyering of any kind will also be changed by AI. In fact, if you ask me, it's going to be one of the first jobs that will be quite heavily impacted by AI, because a lot of, for example, clerical work that was done in a law firm right now, a lot of that will be done by AI in the blink of an eye. Whereas now, sifting through ten volumes of jurisprudence might take couple of days for a legal clerk. Well, AI will be doing that for you while you drink your coffee. That is also going to change radically the profession from inside. The same will happen to courts, and how courts will function. And that in itself will require quite a lot of adaptation. Not that I think that lawyers will disappear, on the contrary. I think lawyers, just like many other professions based on intellectual input, they'll have to learn to use AI tools in their work, adapt these tools for their needs, and then use them for a new dawn of the profession.

Scott Patterson:

Thank you so much for that. Andrew, do you have any questions?

Andrew Lin:

Sure – thank you so much for the very comprehensive interview, we really appreciate it. I have one question, which is the role of private ordering within the future of the AI Act. So I think until now, one way that companies, at least certainly here in the U.S., and I think European companies as well, take on corporate governance within the AI space is through private ordering, defined as figuring out what works best within that individual company.

Given the AI Act and the rules and the regulations that are coming out of the European Parliament, do you think there's still a world in which private ordering is so important? Or do you see a world in which even if it's important, it's greatly diminished?

Dragoş Tudorache:

What is private ordering? I'm not familiar with it.

Andrew Lin:

It's where an individual company comes in by itself to set its own governance standards.

Dragoș Tudorache:

I don't think that will necessarily die away, disappear, or be rendered unnecessary or irrelevant by regulation. I do think that was an effect of the lack of regulation. I think at some point various companies have started to ask themselves, listen, if no one tells me what I need to do, then I need to figure it out myself and put myself some ethical standards in place.

Which in the absence of rules, they served a purpose, and gave some companies at least, an appearance of respectability, because they could say, listen, we have our own norms, we have our own ethical mechanisms. Nothing will stop them from continuing to have them in parallel with rules, as long as it is clear that the rules have to be respected, particularly where the rules are mandatory, as it happens in the EU market. For a while in the US there won't be the equivalence of that. Therefore, I would say that what you call private ordering will be continuing for a while, but certainly I think it will be on a downward trend as more and more jurisdictions will start fixing in law the expectations, the norms, and the rules.

You know in a way, if you look at any other more mature industrial sector, which has gone through what the digital sector is going right now, maybe eighty to one-hundred years ago, it's the same thing. At the beginning, each car company had to figure out their own standards up until we started to put standards in place on how you build the wheel, how you build an engine, what requirements you expect out of a car company in order to ensure safety from seat belts to ABS, and so on, and so forth. All that started one-hundred years ago by being things that each company was doing on its own, up until as society, we decided that it's important that we have standards that would apply to all the same. It is happening now for digital. It is time for digital companies to realize that now they are grown-ups.

Scott Patterson:

Thank you. To reiterate what Andrew said, thank you so much for taking the time. That wraps up all the questions we had.

NEW YORK UNIVERSITY
JOURNAL OF LAW & BUSINESS

VOLUME 20 SUMMER 2024 NUMBER 3

THE EU AI ACT: TOO EARLY AND TOO COMPLEX?

JÉRÔME PHILIPPE*

SEAN URIBE:

I'd like to begin this conversation by asking you to set the scene a little bit for us. Could you please share with us how the most recent AI developments, particularly AI Act, came about in the European Union?

JÉRÔME PHILIPPE:

Thank you, Sean. The AI Act has been under construction for some time, a few years, with quite a number of debates, especially in France but not only. I think there's a relative consensus in Europe on the need to do something.

However, this Act here is a pretty heavy one, maybe too heavy for a nascent industry. It's 272 pages long! It's extremely structured, clearly a bit cumbersome. It's going to create new significant constraints in terms of regulation, debates with regulators, with possible fines in the end.

And, it's also going to create private enforcement activity, I think because it defines many obligations. When you are a client or a subject of AI, you will see that people implementing AI have a number of obligations here. And nothing prevents you, as a third party, a user, or a consumer association, to say:

[*] Jérôme Philippe is a partner in the Paris office of Freshfields Bruckhaus Deringer LLP. He advises clients in antitrust, foreign investment review, data regulation, cyber and national security. He represents his clients before governments, regulators and courts. He is a Non-Governmental Advisor appointed by the French competition authority before the International Competition Network (ICN).

"Okay, I consider you did not fully comply with the AI Act, and the regulator is not acting enough, so I'm going to enforce it by myself. Before a court, based on usual tort law and a violation of the AI Act." We expect a lot of private enforcement coming at some point, maybe not immediately, which will create a lot of litigation. And that's one of the issues with those complex and heavy laws such as the AI Act. We see it today with the GDPR as an example, although the GDPR is much simpler than the AI Act.

All this litigation constitutes a cost. Especially when it comes at the very early stages of development of a very new industry. One of the major questions is whether this regulation has come too soon in the development of AI. Many people consider the AI Act to be at risk of hindering innovation and competition. To sum up, when you see that massive regulation with hundreds of pages all setting obligations, you have the feeling that someone has been thinking: "What are all the possible problems that AI could create? Let me regulate all that in advance."

This approach could raise criticism of course. For example, the French government has been working for months to try and alleviate some of the obligations and make them less burdensome for the players, especially the small players. Those could face barriers to entry partly because of the regulation. There's a French actor for example: Mistral AI. It was recently created in 2023, but already has a very high valuation and is seen as a possible competitor to big players for the next stages. That's definitely a good thing to have young competitors like this. We want to have competition, and of course the Government doesn't want AI to be reserved to the big players that are already installed.

It is in this context that we would need to figure out how this regulation would play out. Is it going to favor competition? Or is it going to create too many obligations that end up being so costly that they create significant barriers to entry? These types of regulations are already very difficult to comply with for big, established players with large legal departments. It will be even more difficult for start-ups or mid-size companies to comply with, especially since when you are a newcomer, legal is usually not your first preoccupation amidst your attempts to making your product work and going to investors and markets.

Another feature of the AI Act is that it is extraterritorial, as it applies not only in Europe, but it will cover providers of AI anywhere in the world, provided that their product is used in

Europe, which I guess should be the case for most AI products. So *de facto*, it's a worldwide regulation that can also create a sort of race to regulation if other countries or regions want to do the same. It's like trade barriers, it's always nice to be the first one to create it but then you have to face replies. Here, this creates incentives for other countries to regulate at the same level too and you end up piling up many regulations from many places, all being *de facto* global. That could be a real issue of consistency and of costs.

Of course there are also good things in this regulation. It's clear that when you see some uses of AI, especially generative AI or foundation models, there can be risks associated with that. In particular, there can be an informational risk of being unable to know what is true and what is not true, what has been made with AI and what is natural and made by man.

So of course, having some transparency and some rules is needed. But it is a matter of level. Here, we have two hundred and eighty or so pages of rules, many of which may require clarification. Thus the publishing of the act is not an accomplishment (even if in reality it is in view of the EU decision process) but it is a starting point. The next years will be about implementing all that.

Entry into force should be a matter of a few months. But then, once it enters into force, all the rules do not apply immediately: you start a period between 6 and 36 months for full implementation. Some parts of it, I would say the most sensitive parts, will start to be implemented 6 months after the entry into force. And for other parts, it'll be 12, 24, or even 36 months after implementation. I think this will create a lot of activity because it applies to new AIs, but also to existing ones. For example, you have an obligation of traceability of the data you use for training high-risk AI. This means that when you have already started to train, you need to get back to what you did previously and track it retroactively. A lot of guides are being published everywhere on what you should do to be compliant. But there will be room for a lot of interpretation too: debates will take place because sometimes these obligations are expressed in broad terms, leaving a lot of scope for clarification and implementation… or litigation.

The European Commission is also supposed to adopt a number of implementing regulations. That will all take place in the near future. National authorities should be appointed, one or two per country, depending on how each Member State wants to organize that. However you will not have massive national implementing regulation as this is not a directive, this is a regulation. It applies directly everywhere in Europe. You don't need national Parliaments to adopt implementing laws except in the specified areas where the AI Act has provided an obligation or a possibility to do so.

Despite this extensive regulation, some of the debates raised by AI are not fully resolved. For example, in France, there is a big debate on how we should apply copyrights. Based on a EU Directive, France was the first in 2019 to implement what we call neighboring rights, which is basically money that platforms like Google, Apple, Meta and others should pay to newspapers when they use their articles, or when their users use such articles in posts, and more generally when they give access to their articles through the platform. There's been big debate on whether those rights were due or not. Lobbying went up to the EU and that gave rise to a Directive that has provided that there should be in some cases a compensation. The Directive does not include AI of course, just social networks platforms. So here now you have a rising debate for AI, and I see that this debate does not only emerge in France and Europe, but also in the US. France has been at the foremost of it to protect the owners of rights on articles, books, and also movies. With a different and older system that also exists for music. Today the new question will be whether they should be paid for the use of their intellectual or artistic production by AI for the purpose of training.

If you think of applying these rules to AI training, the question to ask is what use do you really make of the intellectual or artistic productions when training AI? By using it for training, do you make it available ? Should you pay for that use or not? There is the evanescent idea that this use enables the AI provider to make profit, but how to measure it? There will be litigation and you probably have competition authorities that may want to act also, although I'm not sure they will have such an easy way of acting as they did in neighboring rights. For neighboring rights, the French competition authority was very active. It was the first one to be active in a case against Google. The solution of which was extended to other platforms. So this is something I expect for the future, i.e. debates nationally and at the EU level on compensation for the use of intellectual and artistic data for the training of AI. And this will create another subject within the subject, which is the obligation that will exist on high-risk AI to indicate the data they used for training.

There are two points which I think are problematic for a number of AI providers. One is indicating the data used and sometimes indicating even the source code of it, which is part of the EU regulation. The other is that this will create circumstances that may force you to give indications that are actually your business secrets. Choice and enhancement of training data could be a matter of competition between AI providers. If you have access to better data than others, that's a comparative advantage. In competition law there are very limited cases where you need to give access to essential resources, which sometimes included data but that was not in the context of AI. Apart from those rare cases of data monopolization, if you have a case where there is no dominance nor essential resources and the only thing that data provides is a mere competitive advantage, then its beneficiary should normally not be forced to publish or disclose the data, especially by the government. On the contrary, disclosing in such case could be seen as reducing competition. Therefore these issues of disclosing data and paying for it will most likely fuel a large debate in the future.

If we come back to the AI Act itself, it will cost quite some money to comply with it. It will force all the actors in the chain to take advice, actions and demonstrate at least a minimum degree of compliance with those obligations. This will include a need to precisely define roles.

The AI creates roles: you have the provider, you have the importer, you have the deployer, and the Act gives responsibilities and obligations to all of them. Sometimes it's not very well defined and you may not be able to comply with some obligation. For example, if you are the provider of the AI and you are asked to follow your AI during its life cycle and to provide a number of information. I'm focusing here on what we call high risk AI in the regulation. You have to follow your products and to document a number of things about them, to which you don't always have a direct access. It may be your clients who have access. If there are issues, how do the initial training and the subsequent use of the AI interact, how is the AI amended during its use with, for example, new biases that did not exist at the beginning and that will start to exist during commercial use? This can be so because at some point during use, the system will progressively bias its own output and with the feedback loop will reuse it. What if, similarly, you provide a non-high-risk AI, but your clients amend its use and make it a high-risk AI?

That may make you lose your status of provider but have new duties vis-a-vis the new provider, though you may not even know about it.

Sean Uribe:

Could you explain the concept of "high-risk" within the meaning of the AI Act?

Jérôme Philippe:

The AI Act engages in a risk-based approach. Basically, the heavy constraints are for high-risk AI and foundation models. There is a list of criteria to define high-risk. For example, as soon as the AI performs profiling of persons that has an impact on the persons' rights or duty, you are in high risk. So, it's relatively easy to be considered high risk.

Take, for example, educational AI. That is high-risk in most cases. If the AI is used in an employment relations context, it's very likely high risk too. Moreover, you can very easily fall in the scope of high risk if your AI is embedded in a system that is already regulated.

Reality will certainly show that we need hundreds of additional pages of implementing regulation! I'm obviously not calling for that. But clearly the point is when you want to be so precise in the obligations as the AI Act is, but you're still not 100% precise as to the scope, then you create legal issues.

The regulation is so complex it will create uncertainty. Usually, regulators tend to apply regulations strictly, but they also have to adapt to the situation they face in a clever way. And generally they do it, but it creates significant legal uncertainty for everybody because, you never know how the regulation is going to be interpreted by the regulators especially for a regulation that emerges before the industry has really emerged! And this will be exacerbated by the fact that the regulation is so complex that I expect that no one will be able to entirely comply.

The AI Act is based on the same model as the GDPR in data privacy, but is more complex, and applies to a less developed industry. And yet, when you dig in nearly every company, you always find some degree of GDPR non-compliance. That will be even worse for the AI Act.

So will the regulator understand your situation and take account of it or not? I mean by being benevolent to some extent. That's a big uncertainty, as regulators are not meant to be benevolent.

If one wants to properly comply with the AI Act, he will need to have high degree detailed cooperation with other actors in the chain. As an example, cooperation is requited between the provider of the AI and its deployer. And at some point, there is not a full clarity as to whether the deployer may become provider in turn. Also, it is not clear whether selling a product incorporating AI may impact your role, e.g. by making you a provider.

Additionally, by forcing too much cooperation between the provider and the deployer (i.e. in common terms the user of the AI), you may in some cases end up with competition issues.

For example, if you look at one subject, which is not dealt with here, which is price. As a competition lawyer, when I advise suppliers, I tell them that they are not supposed to know all what their clients do with their own clients: your client buys your products, then they use or resell them and you're not supposed to know to whom and at which price. Once they have bought your product, they are free to use and resell it provided they do not breach the conditions of use and the contract, and you should not try to influence that use. For example, what we call "destination clauses", where the provider attempts to control to whom the product will be resold or with whom it will be used, are often considered to be anti-competitive. Well, with the AI Act, the provider may have no choice but to interact with his client's commercial policy, as that policy may have an impact on the provider's obligations. As an example, although as a provider you did not build your AI product to be a high-risk AI and you did not comply with the additional obligations that this would have imposed, considering your product shall not be high-risk, what if your client starts using is in a way that makes it a high risk AI (e.g. in the areas of education or employment)? Therefore you need to protect yourself from that, but this means interacting with you client's commercial policy. Which, again, you are not supposed to do from a competition law perspective....

ANDREW LIN:

So, on that point, would you create clean rooms, with different trees within so that they don't touch? What would be your advice?

JÉRÔME PHILIPPE:

You're right, the advice can certainly be to have clean rooms in some situations, in order not to share information that is too sensitive. However, it's not very clear how clean rooms would interact with the obligations here because at the end of the day, it's an obligation on the deployer or an obligation on the provider, and you may need to really access the information in order to comply with our obligations under the AI Act.

In particular, if I have the relevant information in a clean room, I may need to have it outside of the clean room too in order to make a full regulatory use of it and to be able to discuss if I need to engage with the European Commission or the national regulator. So I think there are some cases where clean rooms will work, and other cases where they won't. In addition, due to the technical complexity of the matters concerned, you will need to often involve engineers and strategy people in those discussion, which may not go along well with the use of a clean room.

SEAN URIBE:

Thank you so much for the background. Getting more granular, could we talk about the intersection between both the new AI Act, GDPR, and some other existing data regulation regimes such as the Data act? I'm curious to know what your thoughts are about the interplay there and, and potential issues that might emerge.

JÉRÔME PHILIPPE:

In principle, it's very simple. They are supposed to all apply in a cumulative way. But in reality it will be much more difficult to do. I will take an example with the GDPR. There are several legal bases for data processing, one of them being consent by the data subject. When you have consent as the legal basis for a processing, one of the particularities of that legal basis is that the data subject has the right to withdraw its consent at any time and with no explanation. In that case the data controller must remove the person's data and stop the processing.

The point is, how are you going to comply with a withdrawal of consent when the data has been used already for training and so has become part of the AI system? One short answer may be it's no longer in the data set so it's fine. However we do not know whether this is sufficient, as the AI is still working on the basis of a training including that personal data, so is there still some use of it and is it still a personal data?

Of course, one of the possibilities that is mentioned in the regulation is to anonymize data when you train an AI. Your set of data used for trainings remains but is no longer considered to be personal data. However the criteria for valid anonymization is that you cannot infer back and find the person. If you achieve this, then it is no longer personal data and the GDPR is no longer applicable.

However, how sure are you that your data is really anonymized when you are working with AI systems, and are you sure it is not possible, precisely using AI, to infer back who that person is or who that group of persons is?

Indeed, for your model to work well, you generally want the data to be as precise as possible. Thus, even if you remove ID, you will often keep all the "metadata" on the person, e.g. sex, age, region, type of living, tastes, job, family, other characteristics, etc.… How sure are you that you system cannot infer identity back? So, the interplay with GDPR is pretty difficult.

In practice, what we see is that the data protection authorities, although they really enforce GDPR with a strong view to protect data subjects, are also realistic and to some extent may adopt a pragmatic approach, based on what is technically possible and what is not possible. Thus, I would say that at some point we will probably find a point of balance. That will certainly be dealt with soft law. We have hundreds and hundreds of pages of soft law, such as interpretations, guidelines, presentation, and this can give clarity on some points but it also makes the law very difficult to apply without a high level of investment in it.

In relation to soft law, you may have different guidelines from different national data agencies as they don't always fully coordinate with each other to ensure consistency. When you go into the details, you find differences between them. For example, in the way we apply GDPR in various countries, you encounter small differences, which may sometimes become meaningful in the context of a given project.

SEAN URIBE:

It is certainly a very complicated issue. Moving on, I think another question that we are pretty interested in is how you anticipate this new AI regulation to impact the business climate, particularly outside of the European Union.

JÉRÔME PHILIPPE:

Well, first, there will be bad surprises for a number of actors—I'm not speaking about the big players. The big players are already involved in the discussions, and they will be ready for sure. But if you are a smaller player such as a new tech, it will be much more difficult and costly to comply. I will take again my former example Mistral, the young French startup creating new AI products. How are they going to implement such a tough regulation, I don't know, and I think this is an open question. Generally speaking, what we call the French Tech, i.e. the set of innovating tech start-ups, has spoken negatively on the AI Act, which they see as creating a risk that AI research and development work goes to other parts of the world.

But even abroad, as soon as your AI is supposed to interact with European citizens, a first obligation will be to appoint a representative in the EU if you don't already have one. And then, you start piling up obligations, especially if you provide a high risk AI. That is going to make development more costly from the outset. What we should hope is that it'll not create too many barriers to entry with products that you cannot sell simply because you need more money to both develop your product and comply with all this and that again.

This is the first and foremost question – is it going to make it too difficult to develop AI, and thus hinder innovation, or not? Is it going to concentrate innovation on the big players that are already established?

The French Competition authority (the FCA) has rendered an opinion on the AI sector a few weeks ago, in which it expresses concerns about the risk of major digital players engaging in strategies to consolidate their market power upstream of the generative AI value chain and to extend any market power into existing and new downstream markets. In particular, the FCA identifies several risks of abuse, many of which relate to access to key inputs (such as computer/chips, data, talent and capital) as potential high barriers to entry. In light of these concerns, the FCA has put forth a series of recommendations aimed at fostering competitive dynamics within the sector. These include ensuring that the implementation of the AI Act does not slow down the emergence or expansion of smaller operators, and that the largest players do not divert the AI Act to consolidate their market power, though a so-called AI Act "washing", notably through the AI Act exemption applicable to open general purpose AI models.

When you look at the communication by the French competition authority at the time of the launch of that sector investigation, its Chairman said in substance, if I may sum up, we are doing that because we don't want AI to be monopolized by a handful of already established US players. This is the role of a competition authority obviously to ensure that access to the market is maintained, including for newcomers, but the question is whether such a complex regulation on an emerging industry is really the right way to do so.

Additionally, one should always be careful when putting in place such extraterritorial regulation because other countries may respond as well. To some extent it works like protectionism. You are happy for some time when you're the first one to move, but you are less happy when others replicate. Here, I hope this is not going to trigger similar extraterritorial laws in other regions but I fear it will, as this would or will result in piles of competing legislations applying altogether and making innovation even more difficult.

This is an issue of such a complex and extensive regulatory approach at an early stage of the industry. I'm a bit afraid, I must say, and our clients are a bit afraid, that it may well make business more difficult, and at some point, it may slow or hinder innovation.

SEAN URIBE:

Right. Well, fingers crossed those risks don't materialize. We may have touched on this slightly, but can you speak a little more about what you think boards need to be doing right now in order to ensure that their compliance programs take into account these advances?

JÉRÔME PHILIPPE:

All these issues are more and more subjects for Boards of directors, as they are really structuring ones.

It makes me think of cyber risk. Ten years ago, cyber was not a Board level subject. Now it is definitely a Board subject because the risk you face is an existential one. It is the same here, in terms of compliance first, but also in terms of reputation. Reputation and trust are important in the AI world, because AI is at the same time exciting and worrying. If tomorrow you get a name and shame decision saying you did something wrong and that your company is not compliant with the regulation, this may have a cost much higher than the fine, which by the way may already be high.

So compliance will have a high cost for sure, but non-compliance is likely to have an even higher one. That makes it a matter for the Board. This is not only a subject for the regulatory department, or for the public relations one, or for legal. This is a real subject that needs to go up to the Board of Directors and involve the whole company. It is a cultural matter. There is a need to develop and maintain a culture of compliance, and AI will be part of it.

Thus I think the Boards should anticipate the AI Act as much as possible. Now that it is adopted, implementation will be progressive for a long period of time. This gives time to anticipate and start preparing for it. That work should start right now if it hasn't started yet, as implementation will take time. As an example, it is not limited to internal measures, but it will induce changes in contracts with partners, clients, suppliers, etc… All this need to be anticipated and negotiated in advance.

In practice, the Board should appoint an AI Act coordinator, who will be specifically in charge of ensuring compliance, will interact will all the departments that are concerned, will have authority to make the compliance plan progress, and will report directly to the Board.

I would say those persons who will be appointed should be at the right level in the company in order to make sure compliance is warranted in the end, so you'd want someone sufficiently senior in the organization to be able to shape the way the organization will work, because that will have an impact on how the whole organization will work. There will be internal reluctance of course, as compliance with the new act will change ways of working and will add constraints That should be organized with clear Board level indications, on the basis of a strategy endorsed by the Board.

Indeed, it will be essential for an AI to be compliant. For all the high risk AIs, you will have a "CE" marking on the product. Technically I don't know how you mark "CE" on an AI, but joke apart, that will be obviously key for commercialization, and also embedded in other products in Europe.

In particular, if that "CE" marking is removed, it will mean big issues for the product because it will immediately be barred from the European territory. If it's embedded in third parties' products, then you face even bigger legal issues with your clients, with potentially high levels of liability. Needless to say, contracts will need to address that issue very cautiously.

You just have to look at the issues that a company like Boeing is facing at the moment, not in relation to AI though. Just imagine your AI is marked on 10 million cars in Europe in view of ensuring their safety, and from one day to other, it has to be removed what would be the consequences of that ? There is no doubt such issues can become enormous and vital for a company. So, it's a clearly very important subject. Boards should really as soon as possible organize themselves to be able to implement that and reduce risk.

Regarding companies that will embed third parties AI in their products, such as car makers for examples, AI due diligence will be a major subject for safety and quality. When you look at it from a supply chain perspective, it is actually very close to cyber issues. You need to make sure your providers will be compliant and you need to develop you own due diligence ability. At some point you may need to be able to audit what you are going to embark. Either you can do this yourself, but this means developing the ability, or you need to select trusted third parties to do so.

To this extent, it is a sort of "know your supplier" approach, as you could be the first victim of a non-compliance of your supplier. In itself, this may make entry on the AI markets much more difficult, as you will need to be able to prove strong track-records and comfort to your clients about compliance.

And at the end of the day, it may be that the biggest barrier to entry in that industry is how to obtain the trust of your clients. You need to have track records, you need to have a lot of accountability, transparency, and that means it's something difficult when you are a new company. There will be a barrier to entry here.

This is where I come back to my first point on regulation. Is it too early? Is it good here to be ahead of the curve, or could it create a bad situation because, even if there are legitimate reasons for regulating, it comes too soon and you face issues of bias against entry and bias against development.

Finally, we should anticipate complex business relationships and complex liability issues. For example, take a car manufacturer – say it decides that it will integrate some AI into its product, which by the way is or will be a strong market constraint. It may also buy components which themselves may have AI in them. As an example, the radars that certain cars use which are used to safeguard against accidents, these might include AI and are not usually components which are developed by car manufacturers themselves. You will have AI that will reconstitute the environment using data coming from all the (sometimes AI-powered) sensors. And you may have central AI that will manage the vehicle. So, you have several layers of AI products: some developed by the car manufacturer, some procured from third parties for specific tasks, and some already embedded in components that are separately procured. This means multiple stages of AI incorporation in the product, and communication buses between them. And when you are the car maker, you are at the end of the chain. The point is, you need to get visibility not only into your direct suppliers, but sometimes the suppliers of your suppliers. This is something difficult because when that visibility includes how that AI was trained, which kind of data it trained on, et cetera, that makes it exceedingly difficult. And this will be key not only for compliance, but also for the proper functioning of the vehicle and for the determination of liabilities in case of technical issue.

ANDREW LIN:

So, Jérôme, could we dive in a little bit more on the different layers and the lack of visibility. Let's say you are a plane maker, and you're using all these AI technologies. Assume the AI uses data that violates the AI Act but improves safety by ten times. So, here, you have a tradeoff. Do you think in these contexts where the benefits the AI brings are substantial that there will be exceptions to these rules? Where do you think it'll be a per se rule? If you don't meet the guidelines, you're out of the game?

JÉRÔME PHILIPPE:

In theory you don't have such a balance in the regulation. The concept of balance between pros and cons is not in itself visible in the regulation. Thus the short answer should be, if it's not compliant, it cannot be used. If it's on a plane as in your example, it means the plane using that cannot take an EU passenger on board or fly into the EU.

Now I'm an optimistic person and I strongly believe regulators feel a strong duty to protect the people. Thus I tend to think they would agree in principle to work out a legal solution, though within the limitations set out by the AI Act, which they will not be able to move or to evade.

In practice, in such case, you would first need to assess your own risk. You have a self-assessment to make in the form of an impact assessment. Once done, you would have to engage with the regulator and share it with the regulator. That impact assessment is typically the place where you would create yourself the latitude to make the pros and cons balance. What will my AI bring in terms of added security and what are the reason why it may create risks? There may be some risks I can control to some extent, and then I should take steps to control those risks. There might also be risks which I'm not able to control, at least not now. Based on this, a discussion will take place with the regulator, hopefully ending with the possibility to deploy the product while taking all possible steps to ensure its safety. This way, the system would be deemed compliant.

Take as another example the data privacy impact assessments in the GDPR field. The notion there is that it is a self-assessed impact assessment, and this is something that works well in the GDPR context. Essentially, this boils down to making sure you are asking yourself the right kind of questions. What are the benefits, what are the risks? How do I control the risks? Can I remove all the risks or can I mitigate them? Are there other risks I cannot control? Why can't I control those risks? All of this is part of your assessment. If the assessment is properly done, then when it's reviewed by an authority, you have a possibility to reach a consensus and have it approved by the authority.

Apart from the risk control itself, there are other components of compliance: you need transparency, you need traceability of training data, etc.… Those are mainly processual and will be seen as obligations of means for compliance.

Therefore you distinguish two parts for compliance: a processual part that will not be subject to negotiation, and a substantive part where an impact assessment will be the tool for a discussion with the regulator.

As you can see, there is still a lot to build and limited time to do so. This is why compliance work should start now with strong Board involvement and support. On the regulators' side, once they are appointed by the Member States, there will be a huge amount of work to get to a level of in depth understanding of that regulation that will enable them to apply it rightly while still finding the degrees of flexibility that will be necessary to adapt to an evolving and still nascent industry without impeding innovation.

NEW YORK UNIVERSITY
JOURNAL OF LAW & BUSINESS

VOLUME 20 SUMMER 2024 NUMBER 3

NAVIGATING RECENT EU REGULATIONS ON AI: AN ADVISORS PERSPECTIVE

NICK WOLFE*

DANIEL VENETUCCI:

In a very broad sense, what are some of the considerations you have been looking at from the antitrust perspective, especially in the most recent AI regulations that have come out?

NICK WOLFE:

First, I would place it in context and note that over the last decade, there has been a change to a harder enforcement environment. Particularly in the area of merger control, where there has been both legislative change and more assertive enforcement.

There were many transactions over the years involving the high-tech industry that were largely not captured by the merger control thresholds at the time. An exception was the UK, where the Competition and Markets Authority (CMA) has always had scope to assert jurisdiction under UK legislation even if the parties had little revenue in the UK. It really started to flex that capability in the late 2010s. With Brexit, that held particular importance because the CMA also acquired the vires to review deals which had fell to the European Commission to review on the UK's behalf when the UK was an EU Member State. Before

* Nick Wolfe is European Counsel in the Brussels office of Skadden, Arps, Slate, Meagher & Flom LLP. He is dual qualified in England and Wales and before the Brussels bar and advises on antitrust law, in particular before the European Commission and the Competition and Markets Authority.

then, most regulators weren't really looking into these deals or if they did, they did not object to them or they got comfortable with them based on market feedback and remedies or commitments offered by the parties. I'm sure you've heard people refer to Facebook-Instagram or Facebook-WhatsApp as examples of mergers that did not elicit much regulatory interest at the time, but which regulators have since said they should have reviewed more carefully.

Greater regulatory monitoring has subsequently come about in all sorts of ways. Here in Europe, the European Commission has tried to make greater use of Article 22 of the EU Merger Regulation. This was originally conceived of in 1989, when the EU Merger Regulation was introduced. Not all members of the EU had their own merger control framework, and Article 22 was there to allow Member States to refer deals to the European Commission for review. The idea was to address situations where a Member State wasn't able to review something by itself because it lacked the relevant local legal basis, and at the same time the transaction didn't meet the technical financial thresholds to be subject to review at the EU level.

But Article 22 withered on the vine because most Member States did develop their own domestic regimes. The Commission controversially pressed it into service again in recent years as a route to review these deals where the parties didn't meet the EU level thresholds for review.[1]

Separately, the European Commission has ramped up enforcement, particularly of what they view as large tech platforms. And so has the CMA in the UK – I worked on a case, PayPal-Zettle in 2018, which the CMA reviewed (and cleared), even though the target had very small revenues in the UK. Over the last five or six years, you've seen an enforcement environment where the regulators have said, "we need to scrutinize more closely large tech companies, and we're going to make sure that we can get the jurisdiction to do that, or we will assert our jurisdiction if we weren't really doing so before." As I mentioned earlier, Brexit had an effect here, because the CMA became an additional significant regulator with the flexibility

[1] In September of this year, however, the European Court of Justice in the *Ilumina/Grail* case held that the EC cannot review a transaction if the member state making the referral request has national merger control rules but its national thresholds are not met. Joined Cases C-611 & C-625/22 P, Ilumina v. Comm'n, ECLI:EU:C:2024:677.

to review deals, even ones that involved companies with very modest turnovers.

Looking now at AI, the thing that's really prompted a lot of regulatory activity in the last six months is generative AI. Because clearly AI has been with us for a while, and it's really this ability to generate novel content and provide it via an accessible and user-friendly interface that has excited people, led to rapid adoption and generated a lot of regulatory scrutiny as a result. The European Commission has sought information from companies who have foundation models or use those models to enhance an existing product.

So, the Commission – and also the CMA in the UK over the past year – has already been approaching many companies to ask them: what agreements do you have in place with foundation model providers? What are you thinking to do with generative AI? How is that going to feed into the products and services you offer? What are your ambitions for using generative AI or AI more generally? What are your concerns? These questions relate to the various issues the regulators are looking into, in particular things like whether certain inputs are critical and who controls access to them, what roles do new versus established players play and will existing positions be reinforced, and will there be choice, transparency and accountability that will reinforce the competitive process.

The regulators are at a fact-finding stage at this point, seeking to figure out what the landscape looks like. Of course, the ability to fact find is a valuable part of their toolkit.

Moving away from fact finding, another item in the EU's regulatory toolkit is Regulation 1/2003 Article 8(1). This enables the Commission to apply "interim measures". If the Commission has evidence of a prima facie case of a competition law infringement that will cause irreparable damage – for example, the Commission alleges that there has been an abuse and a market is about to tip, and as a consequence others will struggle to compete – the Commission has this Article 8(1) interim measures ability to approach a company and say they're imposing interim measures. The Commission must open proceedings under Article 2 Regulation 773/2004 and send what is called a statement of objections ("SO") to the prospective addressee of the interim measures, and grant access to the Commission's case file. The recipient of the SO has a right to be heard in an oral hearing and reply in writing. The views of third parties who show sufficient interest to be heard should also be considered.

The Commission made use of interim measures in the Broadcom case in 2019. Broadcom produced chips for television set top boxes. The Commission investigated exclusivity provisions in Broadcom's contracts. The Commission also used interim measures more recently in Illumina-Grail, because Illumina and Grail closed their merger without having received merger clearance from the European Commission. The Commission doesn't use interim measures very often, but I mention it as an example of something that is definitely at its disposal as an enforcement tool.

Another significant development came in February and March of this year. We've seen the Digital Services Act and the Digital Markets Act come into force. I worked as a financial services regulator before I became a lawyer, back in the 2000s. We're very familiar with a world where large systemic banks are supervised closely by regulators who every day get reports from these banks or large insurance firms. And they talk to these banks and insurers about their capital position and whether they're at risk of a run or somehow not being able to do what their policyholders or their customers expect.

What we've seen with the Digital Services Act (DSA) and Digital Markets Act (DMA) in Europe is a world where the European Commission is moving to close supervision of what it deems to be systemically important platforms, referred to as "gatekeepers" under the legislation. The Commission identified six companies. If you're a gatekeeper, you're now subject to a degree of supervision and also reporting obligations – having to send compliance reports to the Commission.

The DMA and DSA oblige those subject to them to give the Commission information on a regular basis, such as annual reports on compliance with conduct obligations relating to things such as use of end user data and terms and conditions imposed on business users, and for DMA gatekeepers an independently audited description of changes made to their core platform services that could affect things such as interoperability. All of this can help the Commission understand what they are doing including in the AI space.

They also have to notify the Commission of M&A in the digital sector, including acquisitions that may give access to new sources of data. This may not ultimately lead to a formal antitrust filing, but the Commission gets a view of the activity that these companies are engaged in, in the M&A space as well as their day-to-day ongoing business, and may require a filing for example pursuant to Article 22 of the EUMR.

There's also the Digital Services Act, which is not really so competition focused. It's more about protecting end users – making sure that harmful content is regulated. That applies to significant platforms or search engines, and there are seventeen large platforms that are covered by it. So, that casts the net more widely and is another way in which the Commission can gather information. In particular, companies must prepare risk mitigation strategies for their platforms.

You mentioned the AI Act, and that hasn't entered into force yet. It's still to go through the legislative process, but the Commission is trying to encourage people to already voluntarily comply with it through the "AI Pact" initiative. The AI Act, as I understand it, is really speaking to the big picture concerns that are talked about in the news – such as "is AI going to take over", this kind of concern that one sees being expressed. The Commission has said that the goal is to support the development of trustworthy AI, to ensure that AI systems respect fundamental rights, safety, and ethical principles.

So, overall, I think the Commission is pretty well equipped to regulate and potentially enforce to address its concerns. But I will also say – to make an obvious point of course – that this is clearly an area where there's a lot of uncertainty and nobody has a crystal ball as to how things will unfold.

Generative AI is a new and dynamic kind of space, and when you have that kind of uncertainty – well, even when you don't have uncertainty – it's difficult for a regulator to reach the perfect biting point for its regulation and figure out that this is exactly how it should regulate something. A regulator wants to avoid under regulating; wants to avoid over regulating; wants to get it just right. Even in normal circumstances when dealing with very familiar territory, it's difficult for a regulator to do that, I think. With generative AI, it's uncertain territory. It's new, and people are still figuring out what it can do, so it's very hard for regulators to get it right and to pitch regulation at just the right point.

That's why they're doing all this fact gathering that I mentioned; that's why they're sending out information requests. That's why they are issuing reports, such as reports the CMA issued in September last year and April this year. They're doing all of that to inform themselves and then make sense of the situation.

Daniel Venetucci:

You've mentioned all these different tools that regulators have to help regulate AI. I'm wondering if you have any sense for how the regulators themselves are utilizing AI to perhaps aid in their enforcements, or simply monitor companies.

Nick Wolfe:

I have fairly limited insight into that. What I will say is they have ramped up their capabilities in the area of forensic science and document review. I guess that's particularly pertinent in a world where companies generate very large numbers of documents, and nobody can humanely go through those. So, the use of technology to bring that to a more manageable state of affairs is obviously very useful, and it is clear that the regulators have invested in this area.

The European Commission has in the past used patent analytics software in order to assess innovation in an industry and take a view on the impact of a proposed merger on innovation, based on patent analysis.

When Brexit happened, the CMA talked about the resources it was spending to prepare itself for an increased work-load. That ranged from hiring fifty more people, to beefing up the technology used by its forensics unit. The EC has also spoken of its use of algorithms to detect where markets may be performing sub-optimally and to investigate whether this may be the result of anticompetitive practices. Recently, the European Ombudsman, which holds the Commission and other EU institutions to account, has written to the Commission to ask how it decides on and uses artificial intelligence (AI) in its decision making. It has specifically asked about the automation of tasks, decision making concerning the use of AI, transparency of how the Commission takes decisions on AI use, and accountability.

Daniel Venetucci:

I want to turn now to more of the business side and perspective. Maybe just in a broad sense, what are some issues that clients or businesses in general are thinking about in terms of AI? For example, implementing that into their own business and potential pitfalls such as driving anti-competitive behavior with the AI.

Nick Wolfe:

A number are looking at how they can use foundation models to enhance existing products or services. And I would say in terms of pitfalls, businesses are very conscious that this is a hot topic for regulators. Even if they haven't been a recipient of an information request themselves, they're aware of the high degree of regulatory interest. So, I think they look to us for guidance on what may or may not be acceptable from a compliance perspective, what good practice looks like and how to approach compliance so that you are doing the best you can from a regulatory compliance standpoint.

Arguably, AI doesn't really change what the concerns might be from an antitrust perspective. Things like foreclosure provide a framework for regulatory analysis – if you take for example a particularly powerful foundation model and someone is also active in providing services downstream that interface with users. The question becomes "What might be the concern if we have a foundation model, and we also have products downstream? What might the concerns be from a regulatory perspective?"

So, one can think about the risk of a regulator investigating potential foreclosure of others who might want to use your foundation model, and questions that may be raised about the contracts you have with customers who use your foundation model (and whether you have overly restrictive clauses in them). More broadly, I think people are aware that if you really boil it down to what the regulators are concerned about, they're concerned about contestability.

If you are active in AI, you may be on the receiving end of a lot of attention from the Commission because the Commission is asking itself questions about the position that those developing foundation models might occupy in future years. I think the CMA said that in an ideal world, we'd probably have multiple foundation models that compete. There are a lot of foundation models out there, and the regulatory query is whether and when they will consolidate.

In Europe, there is a consciousness that we don't really have an equivalent of Silicon Valley, and that some European startups have been acquired by US companies. There's an awareness of that amongst regulators, and they're considering whether there's a way to perhaps prevent that from happening in the AI space. And that explains, for example, the fact that the Commission publicly said that it was interested in partnerships in the AI space, including where an existing tech company enters into a partnership with a newer / startup company.

With the DMA really coming into force earlier this year, we've seen a reaction and it has been in the news, for example, that some companies have made changes to terms or product offerings. So, in case of doubt businesses will look to take advice on whether there are likely to be antitrust or other regulatory issues with their business proposals. The CMA has identified as potential concerns things such as control of critical inputs, bundling potentially distorting consumer choice, and partnerships or investments reinforcing market positions.

DANIEL VENETUCCI:

I wanted to follow up on something you said earlier. You mentioned some ways that it's very easy to apply traditional antitrust principles and analysis to AI. I was wondering if you perhaps thought there was any way in which AI is new and antitrust may have to adjust and adapt to this new kind of industry that's popping up now.

NICK WOLFE:

What I would say to that is that in recent years, the concept of ecosystems has been at the forefront of regulatory analysis in a number of cases. People debate how you define an ecosystem, but an ecosystem boils down to having some allegedly very important assets or dominant product or service. I would emphasize *potentially* – it's for the regulator to determine. But being perceived to have that and then having other services that are within the hinterland of the allegedly very important or very successful product or service. What I've seen in cases I've worked on in recent years is that regulators haven't just reached for traditional foreclosure theories or horizontal concerns, but they've also tested ecosystem theories.

In the AI space one could imagine a regulator pursuing an ecosystem theory of harm, alleging that a strong foundation model could advantage other areas of a business.

There is also potential for regulatory concerns about walled gardens. The DMA seeks to address such a concern by requiring portability of data and so on.

The so-called ecosystem theory of harm has been on the agenda for a few years now. It's been applied in merger cases by the CMA in the UK, by the European Commission in Brussels, and I think by the DOJ and the FTC. And it seems very likely that regulators could apply it in respect of AI.

Daniel Venetucci:

Does anyone else have a question they'd like to ask before we start to wrap up?

Scott Patterson:

I can ask a question in relation to that topic. If clients are concerned about foreclosure, are they also concerned about having to export or send out their data in order to help train other AI models based on the regulations?

Nick Wolfe:

I've not been on the receiving end of a request about something related to this, but it is clear that there are questions about the use of data in training foundation models. Note that the DMA also has obligations on data portability for business and end users, as does certain provisions of the GDPR.

Scott Patterson:

Is portability similar to making it available to everyone?

Nick Wolfe:

So, with foundation models there are both open and closed models. There's a lot of regulatory scrutiny and regulators are asking questions about both. Regulators surely understand that closed models have a lot of benefits. With the closed models, part of the incentive of those who develop them is surely to earn a return on the engagement and investment that they are making. Regulators may seek to set some parameters around how data is used. There are also consumer welfare concerns about data, so I can see that from a non-competition perspective that there will be scrutiny of this. The Digital Services Act in the EU is something that may be useful in tackling that, because that's also about regulating potentially harmful content and also enabling users to understand what their data is being used towards.

Daniel Venetucci:

I wanted to start to wrap things up. Europe has been one of the first major movers on this, and specifically in the antitrust space, so many of these companies are large multinational corporations. And I was wondering with Europe being the first to move, do you think other countries are going to also move to adopt something similar, or maybe something more restrictive? How do you see this playing out going into the future?

NICK WOLFE:

I do think it's inevitable that regulators and other competition regulators in other parts of the world will look at what's happening in Europe and then think about how to develop their own law and their own regime in this space, if they're not already doing something. We've seen this happen before with the increased scrutiny of platforms. That is an example where once it started, other regulators started looking into these cases as well. Within Europe, the Commission really started to scrutinize large tech deals and so did the Austrian regulator, the German regulator, and so on, all essentially looking to exert greater scrutiny either at the EU level or a Member State level.

In my day-to-day work, I think of the major regulators as the FTC and the DOJ, and SAMR in China. And then here in Europe, you have the European Commission here in Brussels and there's the Competition and Markets Authority in London. These are the most active regulators and one expects that what they do is picked up by others around the world, and we may see other antitrust regulators taking an increased degree of interest and governments legislating to provide for new powers for authorities throughout the world.

Ultimately AI is fundamentally a global phenomenon, of course. The shift in economies over the last 40 years or more has been towards transferring bits of information across the globe. That was not the lion's share of economic activity and not what the most geographically spread companies were doing before. They might have exported raw materials or manufactured goods, and mostly they weren't transmitting information across borders, which can happen very quickly. You know, it happens in a second. It would be surprising in such a world if you only have a subset of regulators who were really interested in key aspects of this economy, including AI, because it's part of this very global, very easily transmitted kind of activity. So, it's incumbent on all of the regulators to ultimately get up to speed in this area.

NEW YORK UNIVERSITY
JOURNAL OF LAW & BUSINESS

VOLUME 20 SUMMER 2024 NUMBER 3

THE EU'S APPROACH TO ARTIFICIAL INTELLIGENCE REGULATION

LAUREN CUYVERS* & TONI PITESA**

Note: This interview took place in March 2024 before finalization of the EU AI Act and other potentially relevant legislation mentioned in this Article and any comments by interviewees should be interpreted accordingly.

ANDREW LIN:

To orient ourselves with everything that's going on, could you begin by talking about what was happening two or three years ago? There has been a lot of legislation coming out of Europe. To name just a few, we have seen the Data Act, the Data Governance Act, and then the AI Act. There's a lot going on here. What do you think was the precursor to the AI Act? And what are some of the concerns the European Commission was trying to address with the AI Act?

[*] Lauren Cuyvers is a senior managing associate in the Brussels office of Sidley Austin LLP. She focuses her practice on compliance, regulatory enforcement and litigation related to EU data privacy and cybersecurity laws, including the EU GDPR, EUDPR, ePrivacy Directive, NIS2 Directive, CER and DORA.

[**] Toni Pitesa was a managing associate in the Brussels office of Sidley Austin LLP. He focuses his practice on various aspects of EU law and EU competition law, including merger control and abuse of dominance investigations.

LAUREN CUYVERS:

The AI Act was proposed April 21, 2021, by the European Commission. The EU has always been a more regulation-heavy region and jurisdiction. Looking at all of the different technologies that are coming out, especially AI, the EU was seeing risks to values it holds as important, such as democracy and the democratic process, the rule of law, and fundamental rights privacy. They felt it necessary to issue more regulation to protect those values. The AI Act is a cornerstone piece of regulation for that purpose.

That said, I don't know that we necessarily expected for them to issue this much regulation. As you mentioned, we have the Data Act, the Data Governance Act, and the European Health Data Space Regulation Act. Some of the regulations have been modeled after the GDPR, and the EU is trying to leverage the same Brussels Effect for the laws that the GDPR has had. The GDPR has influenced a number of other data protection laws in other jurisdictions, South America in particular. The GDPR is an important cornerstone because of the importance of data for AI systems—they live and breathe data.

ANDREW LIN:

The AI Act itself is quite comprehensive. There's a lot going on, and it tries to anticipate a lot of different use cases with AI, generative AI, etc. Do you think that the timing in which the AI Act has come out is appropriate? Do you think the law is ahead or behind the technology?

LAUREN CUYVERS:

A law that's trying to regulate technology, like AI, will always be behind the technology, because the legislative process, especially in the EU and perhaps similar to in the US, takes time. When the Commission proposal came out in 2021, generative AI didn't really exist. It started with ChatGPT around November, 2022. As a result, the EU modified the Act to take into account generative AI.That goes to show how important the AI Act is for the EU. The EU also wanted to show the world that they are a pioneer in this space and in a prominent position in regulating it all.

However, some commentators say that the AI Act is actually going against innovation and that the EU will not be able to attract the AI companies that it wants to attract because of the heavy regulation. So, it is a bit of a balancing exercise.

Generally, I think regulation will always be a bit behind technology. But the Commission has been putting in a lot of effort to making sure the regulation comes out at the right time. The adoption was originally planned for April, but they moved it up to March 13, just last week. I think it really shows that they wanted to get this out as soon as possible.

Andrew Lin:

I want to dive deeper on the competition issue. If the purpose of the AI Act is in part to make sure there's enough competition, how do you think a startup or smaller company without the large legal team will fare given that they might find it harder to comply with the regulations? That seems like an additional hurdle to competition.

Lauren Cuyvers:

The AI Act cuts both ways. On the one hand, the regulations are trying to incentivize competition by making sure that everyone is on a more level playing field in terms of access to data because currently the big data pools are with the big tech companies. The Digital Markets Act is a good example of that. On the other hand, the regulations lead to the inevitable consequence that startups will be a bit disincentivized and disadvantaged because they will have to seek legal counsel to comply with the new regulations.

Toni Pitesa:

It also depends on what the startup does. If it's not high risk, then the level of regulation companies have to face is lower. The regulatory burden is not the same for every company.

Andrew Lin:

The wording in the Act is quite broad, so if you're using personal data, you can be high risk. Anything that touches PII or impacts financial wellbeing can be high risk. So how do you think about the legislation as it relates to risk and risk-levels?

Lauren Cuyvers:

The PII processing and access to that data will still be regulated by the GDPR. The AI Act doesn't directly say that if you use PII, it's automatically high risk. It assesses things more on a use case basis. For example, you could be high risk if you use AI in the context of a medical device or to assess someone's credit scores for financial purposes. Another example is that if you use AI in employee recruitment, it can affect whether someone gets a job or not. So in that context, it may be high risk.

ANDREW LIN:

Thinking about the interactions between the GDPR and the AI Act, AI runs on data, and data is regulated by the GDPR. If someone doesn't want their data to be used, but that data is already being used on the algorithm, how would the AI Act address that? Does it consider the technical complexities of rolling back data?

LAUREN CUYVERS:

What you're talking about is if an individual were to ask for all his or her data to be deleted, or object to the processing of their data by AI, how would that trickle down because the data is already being used. This is regulated by the GDPR, in the form of data subject rights requests. Dealing with data subject access, data subject deletions, right to be forgotten and all those rights in our GDPR and other laws is a struggle for many companies.

If the data is fully anonymized, within the meaning of the GDPR, it would no longer be subject to the GDPR and therefore companies may prefer using fully anonymized data for AI processing only.

ANDREW LIN:

But even if you anonymize the data to the point where individuals cannot be re-identified, if the model has enough attributes (as models often have many) such as gender, race, occupation, income, neighborhood, you may have enough datapoints to still triangulate a specific individual. How is that addressed?

LAUREN CUYVERS:

The GDPR has a very high threshold for regarding data as "anonymized". If there's even the slightest possibility that someone is re-identifiable based on linking attributes, then it is considered identifiable and not anonymized.

The issue is that the GDPR doesn't define what anonymization is, so it's largely being interpreted by courts and regulators. We, lawyers, have to look at all of the guidance and core decisions to advise and argue what is considered fully anonymized because it's not very clear at the moment.

Andrew Lin:

Shifting gears, let us turn to the effects of AI in shaping the competitive dynamics. What roles do you see the different AI and especially generative AI regulations have in driving competitive behaviors?

Toni Pitesa:

There's a lot going on in this field right now—in particular regarding the interaction between AI, competitive dynamics and EU competition law.

Depending on who possesses the technology and how they use it, AI can spark pro-competitive effects or anti-competitive effects. The AI Act captures the dichotomy of pro-competitive effects vs anti-competitive effects quite well. Recitals n. (3) and n. (4) explain how AI can contribute to a wide array of economic, environmental and societal benefits across industries and social activities. But at the same time, depending on the application, AI may generate risks and cause harm to public interests, like competition.

In terms of pro-competitive effects, we can look at AI in terms of increased competition, transparency in markets, and better quality of products. For example, when you are looking for flights or hotels, you already have websites relying on AI that can give you a hyper-personalized offer showing you the best time to book your flight or hotel at the best price. This has a significant impact on competitive dynamics and ultimately benefits consumers.

In terms of anticompetitive effects, the malicious use of AI technologies can lead to competition distortions and consumer harm. In the EU, we categorize anticompetitive conduct through two main provisions: Article 101 of the Treaty on the Functioning of the European Union (TFEU) which regulates collusive agreements, and Article 102 of the TFEU which regulates abuse of dominant position.

As regards the application of Article 101 TFEU, one of the main issues is so-called "algorithmic collusion". It is currently still more of an academic topic in the EU. So far, we haven't seen cases concerning algorithmic collusion in the proper sense of the term, i.e. algorithms *autonomously deciding and implementing* an anti-competitive agreement. What we have seen however are algorithms being used to *facilitate* anti-competitive conduct. For example, in a cartel, brands decide the prices they want to collude on and they can use an AI-powered price tracking tool to implement or monitor deviations from the cartel arrangement. We already have examples of this type of cases. Already back in 2016, the UK Competition Authority imposed fines on two online retailers of posters and frames who used an automated re-pricing software to implement an agreement not to undercut each other's prices when selling on Amazon.co.uk. Similar cases have been pursued by the EU Commission as well.

Proper algorithm collusion is still a dystopic scenario that will probably emerge sometime in the future. But this does raise some interesting questions: can you actually attribute liability for what the algorithm is doing to the company that is using it? Can you have an anti-competitive agreement, often requiring the existence of concurrent wills, between machines? For example, if two algorithms adjust prices with no point of contact or interaction among themselves, it would be very hard to prove the existence of an "agreement" within the meaning of EU case law. Because AI acts autonomously, there would be only independent price adjustment, which, in principle, would not fall within the scope of Article 101 TFEU.

In relation to Article 102 TFEU which regulates abuse of dominant position, AI-related infringements could result from the control of key AI inputs (e.g., data, computing hardware, foundation models) by a handful of powerful (i.e. dominant) companies that may decide to, e.g., refuse to supply such input to their competitors, or to provide it under discriminatory terms or for an excessive price. In the EU, we have not seen thus far abuse of dominance cases concerning AI markets (e.g. market for foundation models) but we have seen cases in which the abuse of dominance was perpetrated in non-AI markets (e.g. general internet search) through the use of an AI tool, e.g., a ranking algorithm.

ANDREW LIN:

Since AI collects data from a wide variety of sources, could taking data be considered communicating with one another? Either by the algorithms exchanging data or a third-party exchanging data?

Toni Pitesa:

That's an interesting question. Under EU competition law, an exchange of competitively sensitive information leading to parallel market conduct is likely to be unlawful. It's hard to say if this would happen in the context of algorithms, but if we suppose that two algorithms, because of the way they are programmed, "decide" to exchange competitively sensitive information with each other (e.g. prices) and, as a result, they end up applying the same prices, that could potentially constitute an infringement of EU competition rules. So, the exchange of sensitive data can play an important role.

Andrew Lin:

Here is a hypothetical—suppose an AI algorithm has gotten so smart that it observes behaviors, prices, and histories from public information you can Google. There is no direct exchange or communication, but you could say it's interacting with the public. How do you think that scenario would pan out?

Toni Pitesa:

It's difficult to answer this question given the novelty of the issues brought up by AI. I would say that we would have to go back to the traditional framework of application of EU competition law. The exchange or collection of information is unlawful to the extent that this information is competitively sensitive, is provided in individualized form and, most importantly, is not in the public domain. If the information is genuinely public, it is equally accessible to competitors and customers and thus it does not normally trigger the application of competition law.

Andrew Lin:

What if the algorithm makers market the software as a way to collude on prices—so there is no contact involved in buying the software but the effect of using the software is price convergence while bypassing infringement?

Toni Pitesa:

The present EU Commissioner for Competition, Margrethe Vestager, stated that companies must be held liable for the tools they use. If the software is calibrated in a way that leads to an infringement of EU competition rules, companies may be held liable for the damage caused. But it's difficult to predict how things will unfold in practice because this is a highly technical area and there are no precedents that we can rely on at the moment.

ANDREW LIN:

In terms of liability, which is what corporate clients ultimately care about, do you think it would be a per se rule or determined case-by-case? For example, if a company did their due diligence, but their AI system is still in violation of the AI Act, what results?

LAUREN CUYVERS:

One has to distinguish (civil) liability from regulatory enforcement. The AI Act as such only regulates regulatory enforcement and action - not civil liability or consumer redress, for example (although there currently is an AI Liability Directive in the making that does harmonize civil redress in relation to AI in the EU). The AI Act is not fault-based, meaning that if a company did its diligence, but their AI system is still found infringing under the AI Act, that is a basis for a regulator to take enforcement action under the Act.

One would first have to determine whether the AI system one is providing or using falls in scope of the AI Act and then whether that AI system is considered an unacceptable, high or low risk AI system. Based on the level of risk the AI system is presumed to have, the AI Act prescribes certain requirements. If one objectively fails to meet those requirements, then one can be faced with regulatory action under the AI Act. Non-compliance with the AI Act can expose a company to fines of up to 7% of global worldwide turnover.

ANDREW LIN:

With all the liabilities and risks that AI can bring, there are obviously benefits as well, such as making consumer products safer. If AI improves product safety by a meaningful magnitude, but is undisputedly in violation of the AI Act, how do you think courts would balance between product safety and the violation?

LAUREN CUYVERS:

First, one thing to note is that the requirements within the AI Act are based on EU product safety legislation. The requirements (for high-risk systems) include monitoring the quality of the AI system after it's been marketed and after it's been placed in the market. You also need conformity assessments and to have a CE marking, so it needs to be checked by EU authorities. Then you need to affix the CE marking on the AI system. These are all requirements stemming from concepts under product safety.

Second, the AI Act does not undo existing EU Product Safety Laws, but instead is actually meant to work in tandem with those laws. Given the AI Act is very new, there are no precedents yet on how national EU Member State and EU courts would tend to adjudicate this.

ANDREW LIN:

From a politics perspective, countries compete for business. Are there concerns that other governments might come up with similar AI acts that might make it very difficult for companies to comply with everything? Alternatively, do you think companies may lobby their governments to come up with their own rules?

LAUREN CUYVERS:

Companies that operate worldwide will obviously have to comply with different regulations. There are rumors that other countries will look to the EU AI Act to develop their own laws. It will be difficult for companies to navigate that very complex landscape. To ensure a workable solution that is somewhat future proof, the approach we try to take is to identify a number of core principles in the AI Act (and other laws and regulations such as those in the UK, US and APAC), such as transparency, human oversight, privacy principles, and cybersecurity that can be actioned and incorporated by companies into compliance programs.

We advise clients to stick to the basic core principles and if necessary, adjust these principles and their underlying requirements in the jurisdictions that they need to.

ANDREW LIN:

Thank you, everyone, for the thorough and thoughtful responses to an incredibly complex issue. Could you provide some parting thoughts?

Lauren Cuyvers:

To wrap up, in terms of themes, the main theme is that there's a lot of regulation and more regulation will be issued moving forward (not just on AI, but other (related) themes as well such as cybersecurity).

Toni Pitesa:

As for the application of EU competition law to AI, it's important to remember that AI, depending on how it is used, can give rise to pro-competitive effects or anti-competitive effects. The latter will normally stem from anticompetitive agreements or abuse of dominance.

What is also important to remember is that, in the EU, we don't have precedents concerning competition infringement in AI markets, like for instance in generative AI or foundation models. We have, however, cases concerning more traditional industries or digital markets where AI already plays an important role and where it has been used to facilitate competition law infringements.

Lastly, it must be noted that AI can also be used to detect competition infringements. The EU Commission and national competition authorities are arming themselves with AI technologies, such as price monitoring software, capable of detecting anticompetitive conduct.