Challenges and Opportunities of the EU's proposed AI Regulation

Artificial and Natural Intelligence Toulouse Institute (ANITI) at the University of Toulouse[1]

Recently, the European Commission published a proposal to regulate Artificial Intelligence (AI)(*1*).[2] This proposal has motivated an intense online debate on the challenges and opportunities brought by AI regulation. On the one hand, the proposal brings to the limelight fundamental questions about the boundaries of Artificial Intelligence. On the other hand, it has the power to create and reshape important markets. Together, the chairs of the Artificial and Natural Intelligence Toulouse Institute (ANITI), have been discussing the challenges and opportunities brought by this proposal. Here are our early thoughts and reactions to this proposed piece of regulation.

Challenging Definitions

What is AI? And when should it be regulated?

Defining what is AI, what is not AI, and when we should regulate it, is a key aspect of the EU proposal. These definitions are important because people and organizations will adapt their behavior depending on whether they fall squarely within the boundaries of the regulation or whether they can sidestep it.

But defining AI is not easy. More than a technology, AI is a broad concept that has been approached through a variety of techniques and methods. In the current proposal AI is defined widely[3], from machine learning approaches to basic statistical methods.

---

[1] *The document was written by Cesar A. Hidalgo with input from Celine Castets-Renard, Jean-Michel Loubes, and was circulated and reviewed by the chairs of the Artificial and Natural Intelligence Institute (ANITI).**

[2] This proposal is based on a recent white paper (*2*) and falls in the context of extending the EU's *digital single market* (*3–8*).

[3] From Annex I: "(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases,

In principle, statistical methods could involve techniques as simple as a linear fit (e.g. a linear regression). If the definition of AI intends to include any statistical approach, then this would effectively be a regulation on the use of any form of statistics, or algorithmic decision making, not just on what is today technically referred to as Artificial Intelligence. If this definition does not intend to include simpler statistical approaches, then, the boundary of what counts as an AI system would need to be further clarified.[4] However, the Commission is showing here the political will to be technically neutral and not to adopt legislation that is too dependent on technology which could be quickly outdated.

It should be added that the AI system thus defined will only come within the scope of the regulation if it has the effect of generating results, such as content, predictions, recommendations or even decisions influencing environments with which they interact.

The second definition of the proposal focuses on when AI must be regulated. Here the focus is on high-risk systems. These are applications of artificial intelligence with the potential to have a large societal impact. These applications include the use of AI for biometrics, AI systems for critical infrastructure (e.g., transportation), or systems involved in people's access to organization and benefits. The latter includes multiple forms of scoring, such as university admission systems, credit scoring, human resource applications, educational and vocational training systems, assignment of public benefits, and administration of justice, among others.

Beyond the definition of AI and that of high-risk systems, the scope of the regulation is limited by other considerations. For example, military applications are explicitly excluded, which is justified by the fact that the military domain is not within the competence of the European Union. Governments could therefore adopt regulations to allow, for example, the use of AI technology (eg facial recognition) for national defense purposes.

The regulations nevertheless prohibit certain practices, such as rating citizens. It also prohibits the use of "real-time" remote biometric identification systems in spaces accessible to the public

inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods."

[4] A more comprehensive, albeit verbose definition, was provided in a 2019 document by the High Level Expert Group on Artificial Intelligence. https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines and by a JRC https://publications.jrc.ec.europa.eu/repository/handle/JRC118163

for law enforcement purposes. However, the text provides for three exceptions for specific crimes: in the event of “missing children; certain threats to the life or physical safety of natural persons or of a terrorist attack; and the detection, localisation, identification or prosecution of perpetrators or suspects of the criminal offences.”

These boundaries are important because people tend to adjust their behavior near the boundaries of a regulation (*9*). For instance, if the definition of AI systems does not include simple statistical methods, but does include more sophisticated machine learning methods, organizations in high-risk sectors may default to using simpler statistics. These methods could be less accurate, and more biased, but in the light of the regulation, easier to deploy and change. If the definition does intend to include all forms of statistics, and this is a regulation not only of AI, but of any form of algorithmic or mathematical form of decision making, then this regulation could impact systems that are already operational (since they would fall squarely within the boundaries of the regulation).

New Duties and Responsibilities for Providers of AI

Regardless of what qualifies as an AI system, we can look at the duties that must be fulfilled by providers of AI.

Providers of high-risk AI systems will need to comply with a number of transparency and documentation requirements, and also, will need to use vetted data to train artificial intelligence systems. Some of these requirements are relatively abstract, such as enabling “users to interpret the system's output and use it appropriately,” while others require more narrowly defined paperwork. For instance, high-risk systems “shall be accompanied by instructions for use” including “the identity and the contact details of the provider,” the systems “intended purpose,” “the level of accuracy, robustness and cybersecurity,” and “any known or foreseeable circumstance, related to the use of the high-risk AI system in accordance to its intended purpose or under conditions of reasonably foreseeable misuse.”

Also the regulation requires AI providers to disclose the use of AI. Title IV starts by asking AI providers to “ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use.” But this disclosure

is again targeted more for commercial applications, since the same paragraph says that "this obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence."

Another area of concern is the use of AI to manipulate images, audio, or video. For instance, Title IV article 52 requires users of an AI system to be informed when interacting with content generated by AI that "appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake')."

The proposed regulation also deals extensively with the need to certify AI systems. Chapter 5 of the proposal describes the steps needed to register and certify AI systems. Under the proposed regulation, AI systems can be certified for periods no longer than 5 years by notified bodies[5]. In fact, each Member State is required to "designate or establish a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring." These notified bodies shall be composed of competent persons, work in confidentiality, and be free of conflict of interests, among other requirements.[6]

Notified bodies, however, may subcontract some of these duties (Title IV, article 34), as long as they subcontract a subsidiary that meets the requirements laid out for notified bodies.

Expected Outcomes and Implications

So what is the expected impact of the proposed regulation?

Regulating technology is important. Over the last century we've seen many nascent technologies evolve into highly regulated industries. Long gone are the days in which aviation involved garage experiments and medicine was sold from the back of a horse buggy. This proposal to regulate AI certainly moves the industry into a space of regulation that is closer to that of more mature industries, such as those who produce medicine, aircrafts, or motor vehicles. But by doing so, the

[5] "A conformity assessment body designated in accordance with this Regulation and other relevant Union harmonisation legislation."
[6] See Chapter 4 of the proposed regulation for a full description of the requirements for notified bodies.

regulation changes the structure and composition of the market players involved in inventing, producing, and distributing systems involving artificial intelligence.

On the one hand, the need for certification may create important new industries. The need to create notified bodies, and the ability of these notified bodies to subcontract some of these duties, will create a new market for organizations involved in certification. These are organizations with enough expertise on Artificial Intelligence to help inform questions such as when an AI system should be deemed “fair,” or how to vet, or provide, a data set that is “relevant, representative, free of errors, and complete.” This will likely lead to the creation of organizations specialized in AI certification, similar to what we see today in the pharmaceutical industries, where multiple Contract Research Organizations (CROs) provide support during the development of clinical trials.

The proposed regulation may also bring clarity to the market, by providing clearer rules for the requirements needed to deploy an AI system, or a product of AI, within the European market. This is in fact, one of the motivations of the regulation, to help people trust and accept AI applications.

But benefits tend to come at a cost. The regulation may also limit innovation, in both exciting and nascent industries, and could curtail European efforts on the bleeding edge of the industry.

The move to a more regulated space for AI is not a move that will affect all actors equally. It is a move that is expected to favor larger actors, with the experience, expertise, and financial shoulders needed to adapt to this regulation. The regulation will also add an important period of uncertainty. We should expect a lag from the moment the regulation is enacted, to that in which the notified bodies are fully operational, and to the time certifications are completed. Until that process is complete, the added cost of the regulation would be unclear, creating an incentive against creating and distributing AI applications for the European market.

Is it the right time to regulate AI? During the last years, the public pressure to regulate AI has been widespread and vocal. Yet, this does not mean we yet understand how to build, evaluate, verify, or certify artificial intelligence systems. In fact, in issues such as bias or fairness, it is well known that it is not possible to simultaneously satisfy multiple definitions of fairness (*10*, *11*), making the certification of “fair” AI something difficult to implement in practice. In fact, we should expect heated debates about which definition of fairness, or which justifications for these

definitions, can or should be used for specific AI applications in the future. Moreover, we are only beginning to understand how people react to machine actions, compared to the same actions performed by humans (*12*). So at this time, the gap between research and advocacy is large. We know more about the presence of problems, than about how to construct the right solutions.

Will this regulation help “level the playing field”? At the moment, the largest players in the AI industry are in China and in the United States (*13*). These multibillion dollar companies will probably be able to adapt well to these regulatory requirements. They have the capacity to create internal legal teams focused on the production of the paperwork and certification needed to deploy their products. They can also develop products in their internal market before bringing them to the EU. These large organizations also have the financial shoulders needed to contract the certification and legal advice industry that will likely emerge with the creation of notified bodies if this proposal becomes law. Similar to what we see today in the pharmaceutical industry, this regulatory environment may generate a market where few large players are able to bring products to market, while smaller players may need to sell to larger players, or partner with them, to enter the EU market.

The proposal seems to be aware of this risk, and tries to develop a countermeasure by providing regulatory sandboxes (Title V), which would allow testing ideas in pre-market settings. It is also a regulation proposed almost at the same time the EU adopted a plan with the objective of pushing innovations and coordinating opportunities and investments among member states. In fact, the EU is not a federation and member states can also decide to invest in AI unilaterally, such as with the 3IA-ANR program in France (from which ANITI is part of). That said, it is also unclear why sandboxes within the EU would be a more attractive place for developing AI pilots than locations outside the EU, with direct access to local markets.

Is this regulation to the benefit of the EU? On the one hand, it can help ensure that AI applications distributed within the EU satisfy the certification and transparency requirements laid out in the proposed regulation. But this added regulation is also likely to push the development of AI applications outside EU borders, consolidating the position of the EU as a net importer of digital technologies. This is similar to what we already observe today when it comes to the web and GDPR. The EU data environment is more regulated, and some people may feel safer due to this regulation. But this regulation has not given rise to European champions in the internet space. In

fact, EU companies are still relatively small in comparison to firms in the US and China in key online sectors, such as search, social, and e-commerce.

A long and complicated relationship

For a long time, people have had a complicated relationship with artificial intelligence. The relationship between artificial intelligence and society has been marked by a succession of AI "summers" and "winters."(*14*) AI summers are periods of intense excitement about the potentials of artificial intelligence. They are usually brought by breakthroughs, such as those embodied by recent advances in machine learning (*15*–*20*). But these summers are usually followed by AI winters. These are periods of desilusion and backlash, brought by frustration and limitations with the new technology in combination with other social and economic forces.

Just like the AI summer that started in the 1950s had become a winter by the 1970s, today we are seeing a similar transition. But this time is also different. AI has left the lab. It is now closer to the end of a road that starts on ideas and ends on products. If that is truly the case, the effort to regulate AI comes at the right time. It is now a mature technology, similar to the one found in other tightly regulated industries, such as pharmaceuticals and automotive. But if the technology is yet too immature, the effort to regulate it may limit avenues for learning and development that require rapid prototyping and testing.

Time will tell us whether the time was right, as we continue to look at the development of AI technology in and out of Europe. At this time, we welcome the effort by the EU to kickstart a thoughtful discussion on the future of AI regulation.

ABOUT ANITI

The Artificial and Natural Intelligence Institute (ANITI) is a center of excellence focused on the study of artificial and natural intelligence housed at the University of Toulouse. It is home to multiple research chairs focused on Acceptable AI, Certifiable AI, and Collaborative AI. ANITI experts work on the development of new artificial intelligence techniques, as well as on how to make artificial intelligence acceptable in society. For more information, visit aniti.fr

*ANITI Chairs (Alphabetical by last name).
Rachid Alami, Leila Amgoud, Jérôme Bolte, Céline Castets-Renard, Fréderic Dehais, Daniel Delahaye, Nicolas Dobigeon, Helene Fargier, Fabrice Gamboa, Serge Gratton, Cesar A. Hidalgo, Bruno Jullien, Jean-Bernard Lasserre, Jean-Michel Loubes, Nicolas Mansard, Joao Marques Silva, Claire Pagetti, Jérôme Renault, Thomas Serre, Thomas Schiex, Louise Trave-Massuyes, Rufin van Rullen.

References

1. Proposal for a Regulation on a European approach for Artificial Intelligence | Shaping Europe's digital future, (available at https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence).
2. E. Commission, *White Paper on Artificial Intelligence: A European Approach to Excellence and Trust* (Europa February, 2020).
3. A. Busson, T. Paris, J. Simon, The European audiovisual industry and the digital single market: Trends, issues and policies. *Digiworld economic journal*, 17 (2016).
4. A. De Franceschi, European contract law and the digital single market. *Cambridge: Intersentia* (2016).
5. N. Duch-Brown, B. Martens, The European Digital Single Market. *JRC-IPTS Digital Economy Working Paper* (2015).
6. S. Schroff, J. Street, The politics of the Digital Single Market: culture vs. competition vs. copyright. *Information, Communication & Society*. **21**, 1305–1321 (2018).
7. C. Castets-Renard, Le Livre blanc de la Commission européenne sur l'intelligence artificielle: vers la confiance? *Recueil Dalloz*, 837 (2020).
8. C. Castets-Renard, *Droit du marché unique numérique et intelligence artificielle* (Bruylant, 2020).
9. J. C. Scott, *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed* (Yale University Press, New Haven, Conn., 1999).
10. J. Kleinberg, J. Ludwig, S. Mullainathan, A. Rambachan, Algorithmic Fairness. *AEA Papers and Proceedings*. **108**, 22–27 (2018).
11. J. Kleinberg, in *Abstracts of the 2018 ACM International Conference on Measurement and Modeling of Computer Systems* (ACM, New York, NY, USA, 2018; http://doi.acm.org/10.1145/3219617.3219634), *SIGMETRICS '18*, pp. 40–40.
12. C. A. Hidalgo, D. Orghiain, J. A. Canals, F. De Almeida, N. Martín, *How Humans Judge Machines* (MIT Press, 2021).
13. K.-F. Lee, *AI superpowers: China, Silicon Valley, and the new world order* (Houghton Mifflin

Harcourt, 2018).
14. M. Mitchell, Why AI is Harder Than We Think. *arXiv:2104.12871 [cs]* (2021) (available at http://arxiv.org/abs/2104.12871).
15. I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio, in *Advances in neural information processing systems* (2014), pp. 2672–2680.
16. Y. LeCun, Y. Bengio, G. Hinton, Deep learning. *nature*. **521**, 436–444 (2015).
17. A. Krizhevsky, I. Sutskever, G. E. Hinton, Imagenet classification with deep convolutional neural networks. *Advances in neural information processing systems*. **25**, 1097–1105 (2012).
18. N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, R. Salakhutdinov, Dropout: a simple way to prevent neural networks from overfitting. *The journal of machine learning research*. **15**, 1929–1958 (2014).
19. I. Goodfellow, Y. Bengio, A. Courville, *Deep learning* (2016), vol. 1.
20. Y. LeCun, L. Bottou, Y. Bengio, P. Haffner, Gradient-based learning applied to document recognition. *Proceedings of the IEEE*. **86**, 2278–2324 (1998).