Regulating AI: A Success Story for the European Union?

https://www.e-ir.info/2020/07/13/regulating-ai-a-success-story-for-the-european-union/

EDUARD HOVSEPYAN, JUL 13 2020

Artificial Intelligence (AI) has in the last few years become one of the most topical subjects among policymakers all over the world. It is developing fast and despite some concerns as to its potential negative implications, it seems that it is here to stay. In this context, states face numerous novel challenges. On the one hand, the race to advancing artificial intelligence and reaping its full potential has become one of the primary political goals of today's global powers such as China and the United States (US). On the other hand, AI showcases the growing influence of multinational corporations and their growing involvement in world affairs. States have acknowledged the need to step up their efforts in adopting adequate strategic documents corresponding to the dynamic development of AI technologies and their potential large-scale impacts in the near future. In this context, the European Union (EU) is pressured to act and focus its efforts and resources in staying competitive with the global superpowers.

Starting with some context; in 2017 China adopted its strategy entitled A New Generation of Artificial Intelligence Development Plan, while the president of the US issued his Executive Order 13859 of 11th February 2019 on Maintaining American Leadership in Artificial Intelligence. The importance of taking action in relation to AI is best illustrated in the Russian National Strategy for the Development of Artificial Intelligence for the period until 2030 where it is emphasised that the implementation of the strategy is a prerequisite for Russia's entry into the group of world leaders in the development and implementation of AI technologies and, as a result, the country's technological independence and competitiveness. The first step by the EU was taken in 2018 when the European Commission published the EU AI strategy Artificial Intelligence for Europe. The strategy proposes 3 main objectives:

1. Boosting the EU's technological and industrial capacity and AI uptake across the economy, both by the private and public sectors
2. preparing for socio-economic changes brought about by AI and by encouraging the modernisation of education and training systems
3. Ensuring an appropriate ethical and legal framework, based on the Union's values and in line with the Charter of Fundamental Rights.

This article focuses on the third main objective, mainly ensuring an appropriate legal framework. The reason for this is its strong connection to the other two objectives and the perceived constraints the EU faces due to its more stringent privacy legislation. In doing so, it will be explained why the EU needs to regulate, the challenges it faces, highlighting the specificities of the GDPR, and the possible solutions.

Why Regulate AI?

The European Commission has already stated its position regarding the need to regulate AI in its White Paper on Artificial Intelligence, which was published on 19th February 2020. The main rationale behind the Commission's position is the opportunity before a future regulatory framework for AI in Europe to create a unique 'ecosystem of trust'. Indeed, machine learning algorithms rely on training sets containing vast amounts of data. Trust in the technology and its controller is required in order to unleash the full potential of the data-driven economy. Thus, enshrining sufficient safeguards into legislation could be seen as an enabler to the implementation of machine

learning and AI technologies. Safeguarding citizens' fundamental rights would prevent the use of intrusive technologies and state surveillance policies. An illustration of the use of AI without proper legal safeguards is the case of the Chinese social score. Such examples apply not only to countries outside of Europe, as many privacy concerns were also raised in France with regard to the proposed introduction of facial recognition ID for all citizens.

Nevertheless, the pros of regulating AI extend beyond the immediate benefits for citizens in terms of safeguarding their fundamental rights. Regulation would ensure a level playing field and pose legal obligations on foreign-based companies conducting business activities on the territory of the Union. This could be an indispensable opportunity for the EU to challenge China and the US's roles as leaders in the field, as it could have the effect of 'exporting' the regulatory framework to other states, similarly to the effect the GDPR has had in the past couple of years. In the very recent GDPR first evaluation report, it is stipulated that the adoption of the regulation has spurred other countries in many regions of the world to consider following suit, setting a global trend running from Chile to South Korea, from Brazil to Japan, from Kenya to India, and from California to Indonesia. Therefore, we might expect that if the EU manages to become the first actor to create an appropriate regulatory framework on AI, this may trigger a similar effect to that of the GDPR.

Failing to regulate would enable private corporations to set the technological standards. This would result in legislators reacting to ongoing technological developments, rather than attempting to control the processes. Indeed, regulating rapidly advancing technologies such as AI is a challenging task. It is hence important for the upcoming EU legal framework to be technologically neutral, which would allow it to accommodate such changes. Even large corporations themselves, such as Microsoft and Google, insist on regulating AI. Regulation undoubtedly would benefit private actors in terms of ensuring legal certainty and avoiding large fines as a result of privacy breaches. A safe environment for developing AI would also provide an impetus for European startups. This could potentially decrease reliance on non-EU digital solutions and contribute to the achievement of European digital sovereignty.

Despite all the benefits of regulating AI proposed above, there are still numerous challenges the EU faces in doing so. Artificial intelligence is a cross-cutting technology that has implications on consumer law, competition law, labour law and antidiscrimination law. However, the most challenging aspect seems to be accommodating AI with EU privacy laws and the GDPR in particular.

AI and GDPR: Possible Conflicts

The GDPR has been a legislative success in terms of providing citizens with control over their personal data and obliging data controllers to keep track of what personal data they need, how long they need to store it for and for what purposes. AI seems to pose difficulties in relation to some of these notions. More precisely, close attention needs to be paid, *inter alia,* to compatibility issues between AI and the GDPR in relation to access to data rights and explicability, purpose limitation, and data minimisation. These issues, among others, have been highlighted in the recent comprehensive study by the European Parliament on the impact of the GDPR on AI.

The first issue pertains to the right of access to personal data held by the controller as stipulated in art. 15 of the regulation. This right also encompasses obtaining information regarding the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing. However, it is left unclear whether the exercise of this right also entails obtaining specific information and an explanation on how the decision was reached as stated in Recital 71 of the GDPR. A difficulty that arises concerns the so-called artificial neural networks. Neural
networks are composed of a set of nodes, called neurons, arranged in multiple layers and connected by links, thus modelling in software how the human brain processes signals. The problem lays in the fact that a neural network does not provide explanations of its outcomes. They are based on so many different variables and conditions that decisions do not follow a rationale that is meaningful to humans. Moreover, it has been proven higher explicability in these models leads to poorer performance.

Second, it needs to be assessed whether the use of AI is compatible with the requirements of art. 5(1)(b) of the GDPR on purpose limitation. According to the provisions of this article, personal data shall be collected for specified,

explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. A practical application of AI would be to aggregate existing personal data and identify overall trends or patterns. Data analytics in this scenario seems to be compatible with the GDPR in light of the exception in art. 5(1)(b) allowing for further processing for statistical purposes.

Third, there seems to be a discrepancy between the requirements for data minimisation in the GDPR (art. 5(1)(c)) and the concept of big data analytics, which is at the core of AI and the data-driven economy. The issues stems mainly from the fact that through AI and data analytics correlations are discovered, which could lead to the inference of new data from vast datasets of personal data.

Possible solutions

The issues mentioned above pose a challenge to EU legislators. Therefore, they need to be addressed in the upcoming EU act on AI. The GDPR has been drafted with technological neutrality in mind. This provides opportunities for flexibility in terms of accommodating AI and privacy requirements. Hence, the upcoming EU act on AI can complement the GDPR, rather than being impeded by it. The most pressing challenge is the one related to explicability. Regulation should complement the GDPR by providing clear rules what type of information needs to be provided to data subjects. Furthermore, the complexity of the provided information needs to be determined – whether it should be understandable for professionals in the field of programming or for laypeople. In order for an automated decision to be challenged, data subjects need to be able to obtain information on how algorithms work. This would allow them to identify any discriminatory variables or other data leading to an unjust outcome. As regards artificial neural networks, the sensitivity analysis approach could be applied as suggested by the European Parliament. It provides for systematic checks whether the output changes if the value of certain input features is modified, leaving all other features unchanged. This way it could be understood what features determine the system's output.

Possible solutions for the issues surrounding purpose limitation and data minimisation could be examined together. The future regulation should step on the GDPR's foundations and distinguish between data used for statistical purposes and for profiling. In terms of purpose limitation, the latter should fall solely under the GDPR. Further use of personal data for profiling would be in breach of personal data protection rules (e.g. using medical data for creating an insurance profile). However, aggregating anonymised data and using it for statistical purposes in order to discover correlations and patterns should be allowed under the condition that sufficient measures are taken against possible re-identification. Similar is the case concerning data minimisation. Nonetheless, it should be noted that using AI to make inferences based on provided data could also amount to profiling or to generating new, sometimes sensitive personal data. This would be the case when, e.g. algorithms infer from social media activity the sexual orientation, health status, political affiliations, etc. of users. Therefore, regulating AI should ensure that personal data requirements are respected, while leaving a bigger margin for aggregating and analysing anonymised data.

Finally, the EU should perhaps consider the establishment of an EU AI authority, as recently suggested by the German Minister of Justice. This authority could set standards and coordinate national authorities while working closely with the European Data Protection Board. Similarly to the new EU agency on cybersecurity (ENISA), it may issue certification schemes and foster cooperation with both EDPB and ENISA. Most importantly, it could oversee and enforce the implementation of the upcoming legal framework.

Conclusion

In conclusion, regulating AI could be seen as a strategic goal for the EU and as a possible success story. Regulation could be the key to providing a level playing field for EU start-ups and larger companies to develop in the area of AI by ensuring legal certainty. In turn, this could result in reducing EU dependencies on non-EU tech providers. The most ambitious goal would be to start 'exporting' legal norms outside the EU. Moreover, it was shown in the article that some of the main limitations to the development of AI in the EU could be overcome. Indeed, the issues mentioned barely scratch the surface and many in-depth studies have been carried out in order to address the numerous challenges. And yet these studies show that problems are solvable. Advancing AI does not necessarily need to be a trade-off between being data-driven and preserving our fundamental rights.

About the author:

Eduard Hovsepyan is an Associate Articles Editor at E-International Relations. He holds a BA in International Relations and an LLM in Law from Sofia University “St. Kliment Ohridski”, as well as an LLM in Public International Law from Leiden University, the Netherlands. His main areas of interest include EU digital policies, the intersection between technology and fundamental rights, and international humanitarian law.