ULP Law Review | Revista de Direito da ULP
Vol. 14, n.º 1
doi: 10.46294/ulplr - rdulp.v14i1.7475

Consultation on The White Paper on Artificial Intelligence - A European Approach

Lusófona University of Porto, Faculty of Law And Political Science (ULP) Comment On COM(2020) 65 White Paper on Artificial Intelligence – A European approach to excellence and trust, and COM(2020) 64 final – Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics

Inês Fernandes Godinho[1]

Cláudio R. Flores[2]

Nuno Castro Marques[3]

Universidade Lusófona

Introduction

From 19 February to 14 June 2020, the European Commission held a Public Consultation on several policy and regulatory proposals that are currently being considered in the area of Artificial Intelligence (AI).

[1] Professor at Faculty of Law and Political Science, Lusófona University of Porto, director of the executive board of the ULP Law Review, director and researcher at Centro de Estudos Avançados em Direito Francisco Suárez (CEAD - Francisco Suárez).

[2] Professor of Private Law (Lusófona University of Porto-FDCP); Executive Board member at *ULP Law Review;* Researcher at Center for Advanced Studies in Law (CEAD: Research Unit: *Law, Life and Technology*).

[3] Professor at Faculty of Law and Political Science, Lusófona University of Porto, member of the executive board of the ULP Law Review, coordinator and researcher at Centro de Estudos Avançados em Direito Francisco Suárez (CEAD - Francisco Suárez).

This consultation was centered on two main documents presented by the Commission: the White Paper on Artificial Intelligence[4] and the "Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics"[5].

The consultation also included an online survey[6], where the central themes of those two documents were covered in a summarized way.

In November 2020, the results of the consultation were presented, as well as the texts accepted for publication[7].

In order to participate in this pre-legislative process, a working group was created within the Faculty of Law and Political Science of the Lusófona University of Porto, which presented a contribution that was accepted and published by the European Commission[8].

The White Paper is centered in one powerful objective which is "to enable a trustworthy and secure development of AI in Europe, in full respect of the values and rights of EU citizens", and for that presents two central ideas considered essential to attain it that are to create an ecosystem of excellence along the entire value chain and an ecosystem of trust that ensure compliance with EU rules, including rules protecting fundamental rights and consumers' rights.

The text that follows is divided in two main parts: Part I is focused on presenting an overview on the three main topics pointed out at the consultation: Excellence, Trust and Liability; Part II corresponds to text of the contribution submitted in the Public Consultation held by the European Commission.

---

[4] White Paper on Artificial Intelligence - A European approach to excellence and trust (COM(2020) 65 final), available on: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

[5] Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics (COM/2020/64 final), available on: https://eur-lex.europa.eu/legalcontent/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064

[6] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68461

[7] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68462 - *Public consultation on the AI White Paper Final report.*

[8] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12270-White-Paper-on-Artificial-Intelligence-a-European-Approach/public-consultation

I. Main Topics

1. Excellence

As to building an ecosystem of excellence, the European Commission proposes several actions at multiple levels, as it is considered essential to guarantee that at all levels of the economy and also at public administrations that excellence is attained.

Therefore, in a first level of action – working with Member States – the Commission refers to the Coordinated Plan that was already prepared together with the Member States, that proposes around 70 joint actions for closer and more efficient cooperation between Member States, and the Commission in key areas, such as research, investment, market uptake, skills and talent, data and international cooperation, and is scheduled to run until 2027. On that level, the action identified by the Commission is to review the Coordinated Plan on AI with Member States in the light of the results of the public consultation on the White Paper.

In another level of action, the Commission acknowledges that the current state of research and innovation in EU is fragmented. It is proposed to focus the efforts of the research and innovation community, being imperative to create more synergies and networks between the multiple European research centres on AI and to align their efforts to improve excellence and to retain and attract the best researchers and develop the best technology. On that particular, a lighthouse centre of research, innovation and expertise that would coordinate these efforts and be a world reference of excellence in AI able to attract investments and the best talents in the field is envisaged and the Commission proposes to facilitate the creation of excellence and testing centres that can combine European, national and private investments, possibly including a new legal instrument.

The ecosystem of excellence is strongly dependent of skills, and that is yet a different level of action identified by the Commission. And on that aspect, the Commission proposes a reinforcement of the Skills Agenda, which aims to ensure that everyone in Europe can benefit from the green and digital transformations of the EU economy. Also the updated Digital Education Action Plan will help make better use of data and AI-based technologies to improve education and training systems and make them fit for the digital age. But at

the skills level the ethical guidelines as an indicative "curriculum" for developers of AI is proposed as a tool to be made available for training institutions and, again, a lighthouse centre of research and innovation for AI in Europe is presented as an instrument to develop and spread excellence in skills.

The widespread of skills to use AI is also the basis for a subsequent level of action identified by the Commission – focus on SMES. Digital Innovation Hubs should provide support to SMEs to understand and adopt AI, and so the Commission considers important that at least one innovation hub per Member State has a high degree of specialization in AI. It is also expressed that the Commission and the European Investment Fund intend launch a pilot scheme of €100 million to provide equity financing for innovative developments in AI.

The partnership with the private sector is another level of action and considered essential, so that the private sector is fully involved in setting the research and innovation agenda and provides the necessary level of co-investment. For that, the Commission will set up a new public private partnership in AI, data and robotics to combine efforts, ensure coordination of research and innovation in AI, collaborate with other public-private partnerships. But AI must also be adopted by the public sector, and for that a level of action is also identified: public administrations, hospitals, utility and transport services, financial supervisors, and other areas of public interest shall rapidly begin to deploy products and services that rely on AI in their activities, with a specific focus in the areas of healthcare and transport.

Lastly, the need for AI to rely on data is put forward as an essential level of action. Securing access to data and computing infrastructures is fundamental as without data the development of AI and other digital applications is not possible. But promoting responsible data management practices and compliance of data with the FAIR[9] principles is mandatory.

2. Trust

In the scope of an ecosystem of trust, the European Commission recognizes that as with any new technology, the use of AI brings both opportunities and risks. While AI can help

[9] Findable, Accessible, Interoperable and Reusable.

protect citizens' security and enable them to enjoy their fundamental rights, citizens also worry that AI can have unintended effects or even be used for malicious purposes. These concerns need to be addressed since lack of trust is a main factor holding back a broader uptake of AI. In fact, while AI can do much good, including by making products and processes safer, it can also do harm. This harm might be both material (safety and health of individuals, including loss of life, damage to property) and immaterial (loss of privacy, limitations to the right of freedom of expression, human dignity, discrimination for instance in access to employment), and can relate to a wide variety of risks. The main risks related to the use of AI concern the application of rules designed to protect fundamental rights (including personal data and privacy protection and non-discrimination), as well as safety and liability-related issues.

Facing this problem definition, the European Commission is of the opinion that the legislative framework could be improved to address several risks and situations.

In the scope of *Effective application and enforcement of existing EU and national legislation* and in order to ensure an effective application and enforcement, it may be necessary to adjust or clarify existing legislation in certain areas, for example on liability. On the other hand, considering the *limitations of scope of existing EU legislation* on product placement, it is important to have under regard that general EU safety legislation currently in force applies to products and not to services, and therefore in principle not to services based on AI technology either (e.g. health services, financial services, transport services), being this an important aspect to address in AI legal framework.

Another important aspect is the *changing functionality of AI systems,* since the integration of software, including AI, into products can modify the functioning of such products and systems during their lifecycle. These features can give rise to new risks that were not present when the system was placed on the market and these risks are not adequately addressed in the existing legislation since it predominantly focuses on safety risks present at the time of placing on the market. A related item identified as an improving necessity derives from the *uncertainty as regards the allocation of responsibilities between different economic operators in the supply chain.* In general, EU legislation on product safety allocates the responsibility to the producer of the product

placed on the market, including all components e.g. AI systems. But the rules can for example become unclear if AI is added after the product is placed on the market by a party that is not the producer.

Finally, in the context of AI legal framework *changes to the concept of safety* are paramount, since the use of AI in products and services can give rise to risks that EU legislation currently does not explicitly address. These risks may be linked to cyber threats, personal security risks (linked for example to new applications of AI such as to home appliances), risks that result from loss of connectivity, etc. As such, the EU should make full use of the tools at its disposal to enhance its evidence base on potential risks linked to AI applications, including using the experience of the EU Cybersecurity Agency (ENISA) for assessing the AI threat landscape.

From these several improvement requiring aspects of EU legislation, the first idea is that there is an effective need for new legislation, directly addressing AI. Thus, the future of the EU regulatory framework should have a clearly define scope in its application to products and services relying on AI. As such, both AI should be clearly defined and the design of the future regulatory framework for (high-risk) AI should include some mandatory legal requirements, such as training data, data and record-keeping, information to be provided, robustness and accuracy and human oversight, with clear liability and safety rules.

In this regard, the best way to ensure that AI is trustworthy, secure and in respect of European values and rules, is, in the delivered opinion, both a combination of ex-ante compliance and ex-post enforcement mechanisms and another enforcement system.

3. Liability

Section 3 of the document requested comments on some of the issues specifically identified in the "Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM (2020) 64". This report, which served to condense several other previous studies, highlights the importance of having an adequate legal framework for the level of liability for damages caused by the use of new AI-based technologies. The current legal framework for liability for damage caused by products is

divided between a set of European standards and non-harmonized national legislation on liability. It is proposed to adopt measures that promote consumer protection and that provide companies with legal certainty and it is stressed that future measures should safeguard innovation and the adoption of new technologies. The report begins by making an analysis (not exhaustive) of the current legal framework (European and national), with the aim of verifying whether the current standards are sufficient and adequate to achieve the intended objectives, or if there are gaps regarding the use of AI. This analysis takes place in two parts: (1) the European legal framework aimed at ensuring product safety, and (2) an overview of the national accountability mechanisms prevalent among member states.

The report concludes by stating that the new technologies (AI, Internet of Things and Robotics) have their own characteristics, which may generate different risks from those of other products in legally protected interests. Among these characteristics, the following stand out: connectivity; autonomy; and reliance on data to perform tasks with little or no human oversight. In addition, the possibility that some of these systems may change their performance based on experience - "machine learning", or through software updates, presents special challenges in determining who is responsible for damages. The report also stresses that the complexity of these systems, associated with the opacity of the decision-making process carried out by algorithms, may raise special difficulties in determining the causal link that determines the occurrence of damage.

It is not considered necessary to create new legislative instruments. However, both with regard to security and liability, the report states that it is necessary to reinforce several of the existing duties, to expand concepts (such as the concept of "product") in order to encompass new technologies based on AI and above all, insert in the current regulatory framework explicit mentions of situations specific to these new technologies (e.g., in the case of a machine equipped with AI with machine learning, whether or not it is subject to human supervision depending on certain requirements).

With regard to liability, the report shows a natural preference for the objective liability model (justified by the risk inherent in new technologies), supported by insurance, in order

to ensure the repair of any damage that cannot be prevented and the confidence in the adoption of these new technologies.

II. Contribution

1. The White Paper rightly points that Europe is well placed to benefit from the potential of AI, namely because, as stated, Europe holds large volumes of public and industrial data, the potential of which is currently under-used. And that is at the central aspect – Big Data – that indeed poses the opportunity and also the challenges that may became perils if not well addressed. In this regard, one of the main problems is distributing human rights and responsibilities arisen from the actions of non-humans. Thus, it is paramount to build up skills regarding AI, not only vertically – as via advanced skills (as by Action 3, p. 7) by masters programs – but also horizontally, creating a common basis of training, both technologically and in social sciences.

2. The importance of ensuring compliance with the fundamental values and rights of EU citizens makes the difference between a successful or a fragmented AI policy. In this regard, orienting AI towards a "principled" AI could imply – to pursue both excellence and trust – the drafting of a Charter of AI, which would include the basic and fundamental principles surrounding AI within the E.U., centralizing such principles (and ethical guidelines) under one document. For example, a general principle of accountability would then have effects regarding both civil and criminal liability.

3. AI development will indeed need scientific basis such as academic centers dedicated to it, public and private funding to AI investigation, advanced technology available to investigation and experimentation, infrastructures capable of supporting AI experimentation, among other requirements. But AI is strongly dependent in algorithms that allow for machine (deep) learning and machine (partial or full) autonomous decisions, as for machine programming and machine training there is a need for a large volume of data.

4. Thereto, it is important to promote and support graduate (citizen level) and post-graduate (expertise level) courses with specific AI approach, establishing a European Resource Center (open-access web page) in order to make available, in a centralized hub, the most relevant and actual academic and scientific materials on the main issues regarding AI (as in a virtual AI library). Such an action – together with Action 3 would be important, since aiming at harmonized legislation on behalf of the Member States regarding AI, harmonized enforcement can only be attained through standard training, building mutual trust between all stakeholders.

5. In our opinion, the lighthouse research centre should have a specific unit, dedicated to the validation of algorithms before their usage by private or public sector entities. This validation unit should test the algorithm and propose any necessary change in order to assure its complete safety and compliance to the existing legal framework. A favorable report from this unit should be a condition for the approval of any new AI based system.

6. Machine learning algorithms may self-adapt in order to circumvent fundamental rights or at least make their breach very difficult to identify or classify. E.g., bias and discrimination have already been identified as a possible problem, therefore, we should expect that a AI system will already act in a way that makes it difficult (or even impossible) to detect if that decision was based in any criteria susceptible of contradicting European principles and fundamental rights.

7. Considering machine learning systems in particular, it seems to us that the cumulative criteria for assessing whether an AI application should be considered high-risk, is neither adequate nor sufficient, taking into account the possibility of AI to self-adapt in order to circumvent its classification in the predefined risk categories. Hence, Independently of certification and risk activities classification, human agency and oversight is always necessary for preventing any misuse of AI.

8. The current coronavirus pandemic showed how important it is the collection of data for public health purposes. Also, for security reasons (e.g. terrorism prevention), all available technology should be put to place.

9. The mitigation of risks should involve taking advantage of existing state entities (for example, to control the collection and use of data) and articulate them with the central supervisory entity for the use of AI technologies. We think that in view of the inherent risks, double-checking (at the European centralized level and national) would be justified.

10. The interplay of AI and Big Data necessarily brings for the discussion the interplay of Competition and Big Data, and not only the interplay of Fundamental (and privacy) rights and Big Data. AI is strongly dependent in algorithms that allow for machine (deep) learning and machine (partial or full) autonomous decisions, as for machine programming and machine training there is a need for a large volume of data. And, even if Europe may possess large volumes of underused public and industrial data, the reality is that in some areas private data will be essential, which poses some competition problems that are not even mentioned in the White Paper.

11. AI can be wrongly used to restrict or distort competition. In fact, it has been widely accepted and already detected situations where monitoring software were used to distort competition, as several Commission´ decisions demonstrate (see e.g. cases AT.40465 (Asus), AT.40469 (Denon & Marantz), AT.40181 (Philips), AT.40182 (Pioneer)).

12. We may well preview that algorithms can use data – such as e.g. price data – to execute attain and even execute autonomous decisions on prices, sales conditions among other competition fundamentals. All of that without any conspiracy meetings for price fixing, market sharing or client allocations, but through competitive software that

"intelligently" find the sweet collusive spot among them using data and analytics in a completely different "behavior" pattern.

13. It, thus, is paramount to establish a legal presumption of fault against the AI developer in case of liability for damages, therefore exempting the burden of proof from persons who have suffered harm caused with the involvement of AI systems. Having into consideration the national differences on the matters of liability for damages, we strongly recommend this subject to be specifically regulated in a future European Regulation on AI.

14. In fact, beyond compliance and ex-post sanctioning (via, e.g., machine liability), criminal enforcement is also to be considered, since there is a real peril of the re-orientation of AI technologies to the facilitation or commission of criminal acts (e.g., fraud schemes via Big Data). Considering such aspects is also paramount to achieving an ecosystem of trust, and the White Paper is lacking on specific orientation in this regard. On the other hand, the White Paper also lacks in orientation as to the use of AI in Law Enforcement – vis-à-vis the protection of fundamental rights of citizens and the limits of said use.

All these aspects were not fully considered in the White Paper and we consider them key aspects that need to be addressed. In fact, those challenges are not future or possible problems but already exist, are real and from the present.