EU White Paper on Artificial Intelligence â€“ getting ready for the future (Part 2)

Mr. ClÃ©ment Dekemexhe
Associate
Clement.Dekemexhe@ashurst.com

Mr. JÃ¶rg Heirman
Senior Associate
jorg.heirman@ashurst.com

Following up on our first article on the EU White Paper on Artificial Intelligence (available here), this second article will discuss (A) the requirements with which high-risk AI applications should comply in the future, (B) the key guiding principles on the attribution of roles and responsibilities under future legislation, and (C) the envisaged next steps of the Commission on AI in 2020.

Introduction

As discussed in our first article, in order to create an "ecosystem of trust" the White Paper envisages a mix between, on the one hand, targeted amendments to existing EU legislation to cater for the specificities of AI and, on the other hand, adopting a new regulatory framework that would exclusively apply to so-called "high-risk" AI applications (the White Paper recommends that AI systems be considered "high-risk" when AI is used in a sensitive sector and when such use is likely to give rise to significant risks).

For such "high-risk" AI applications, the White Paper suggests various legal requirements with which such applications should comply. Given the need to ensure proportionality, these requirements will not apply to AI applications that are deemed to be "low risk".

A. Types of legal requirements

By their very nature, high-risk AI applications pose distinct challenges from a regulatory point of view. The Commission's intention is to encourage the uptake of AI applications by addressing these specific challenges in a new legislative framework. By way of example, it is foreseen that the requirements for high-risk AI applications should comprise the following features:

- *training data:* As data is the fuel of AI, its quality and integrity impacts the functioning and outcome of AI applications. Hence it is key that the data used to train AI applications complies with the EU's values and legislation in relation to, in particular, safety and

protection of fundamental rights. Therefore legal requirements regarding the quality (i.e. data used shall be representative to ensure that all relevant grounds of prohibited discrimination are reflected in those data sets) and diversity (i.e. data used should be broad enough so as to cover all relevant scenarios needed to avoid dangerous situations) of the data used to train AI systems should be imposed on the relevant actors.

- *data and record-keeping*: Accountability and transparency requirements for developers are key to fostering the uptake of AI systems across the EU. In that regard, the White Paper suggests keeping accurate records of (i) the data used to train and test AI, (ii) the programming of the algorithm and training methodologies used to build, test and validate the AI systems, and (iii) the data sets themselves (in certain cases only) so as to effectively assess compliance with and enforce the applicable rules. The records and data should be kept for a reasonable period of time and be made quickly available upon request from the competent authorities.

- *information to be provided*: The White Paper takes the position that information provided in a proactive manner to end-users will help to build a genuine "ecosystem of trust". Therefore, persons who use an AI-equipped product or service should have access to clear information about the AI's system's capabilities and limitations, the conditions under which such systems function and the expected level of accuracy in achieving their intended use.

- *robustness and accuracy*: AI systems must be technically robust and accurate in order to be trustworthy, meaning that such systems need to be developed in a responsible manner with proper consideration of the risks that they may generate. To that effect, the White Paper foresees that high-risk AI systems should be:
    - technically robust and accurate during all phases of their life cycle and deliver reproducible outcomes;
    - able to adequately deal with errors or inconsistencies during all life cycle phases; and
    - resilient against attacks and attempts to manipulate data or algorithms.

- *human oversight*: According to the White Paper, human oversight is required to ensure that AI systems do not undermine human autonomy or cause other adverse effects. The appropriate degree of human oversight may vary from one case to another. For instance, human oversight may take the form of reviewing and validating the AI system's decision prior to the decision taking effect (e.g. the rejection of an application for social security benefits may be taken only by a human) or consist of a human intervention afterwards while the output of the AI system becomes effective immediately (e.g. the rejection of an application for a credit card may be processed by an AI system, but human review must be possible afterwards).

- *specific requirements for remote biometric identification*: The collection and use of biometric data for the purpose of remote biometric identification and other intrusive surveillance

technologies (e.g. facial recognition in public places) carries specific risks for the fundamental rights of citizens. The collection and use of biometric data for the purpose of remote biometric identification is already strictly regulated under the current EU data protection rules and the Charter of Fundamental rights, and the use of such data needs to be duly justified, proportionate and subject to adequate safeguards. Given this topic is highly sensitive, the Commission will launch an EU debate on the specific circumstances and on common safeguards relating to the use of AI for such purposes in public spaces.

B. Addressees of the legal requirements

In relation to the addressees of the legal requirements that would apply in respect of the high-risk AI applications referred to above, there are two main questions to be considered.

First, there is the question of how obligations are to be distributed among the economic operators involved. These include several actors, such as the developer of the algorithm, the producer, distributor or importer of a product based on AI, the supplier of services based on AI and the operator or user of a product based on AI.

The White Paper takes the position that the key guiding principle on the attribution of roles and responsibilities in the future regulatory framework should be that the responsibility lies with the actor(s) "who is/are best placed to address it". For instance, while AI developers are best placed to address risks that arise from the development phase, their ability to control risks during the use phase may be more limited.

This approach will require that different requirements are assigned to different types of addressees given the very different roles that these actors have in the life cycle of products and services based on AI. The obligations on AI developers will focus on the risks that can be addressed while AI systems are being developed, while the obligations on users of AI will target the risks arising when AI systems are being used. This approach would ensure that risks are managed comprehensively while not going beyond what is feasible for any given economic actor.

The second question concerns the geographical scope of the legal requirements. According to the White Paper it is key that the legal requirements apply to all relevant economic operators providing AI-enabled products or services in the EU, regardless of whether they are established in the EU or not. This will ensure that EU-based economic operators are not discriminated against vis-à-vis economic agents operating outside the EU.

C. Next steps of the Commission on AI

By the end of this year, the Commission will present a Digital Services Act which will bring clearer responsibilities and modernised rules for online platforms. A European Democracy Action Plan, a review of the Trust Services and Electronic Identification (eID) Regulation, and the development of a Joint Cyber Unit can also be expected.

In the meantime, the White Paper is open for public consultation until 19 May 2020. The Commission Work Programme 2020 mentions that the legislative initiative, including impact assessment, should be released during Q4 2020.

Please do not hesitate to contact us should you like to discuss any of these issues above. We are also happy to assist if you plan to respond to the White Paper's consultation round.