Ref. Ares(2020)3359964 - 26/06/2020

Commission of the Bishop´s Conferences of the European Union

June 2020

Annex to the public consultation on the White Paper on Artificial Intelligence – A European Approach

COMECE welcomes the general approach of the White Paper on Artificial Intelligence to establish a solid European approach of Artificial Intelligence (AI) grounded in values and fundamental rights as human dignity and privacy protection. It is important to **underline the human-centric approach of AI in the EU .**AI has to serve the common good**. AI has to serve the lives of all human beings**. It has to be considered that human life not only has a personal dimension but also a community dimension - community in its human, universal dimension.

Clear definition of AI

COMECE calls for a clarification of the term "Artificial Intelligence".
Artificial Intelligence must be clearly differentiated from human conduct.
The Christian perspective sees the human person as qualitatively different from other beings, with a transcendental dignity, intelligent and free and capable, therefore, of moral acts.
AI systems are not free in the sense the human person is and, in this sense, its act cannot be judged according to the moral criteria that are applied to human acts.[1]

[1] Statement of the Pontifical Academy of Sciences
http://www.pas.va/content/accademia/en/events/2019/robotics/statementrobotics.html

The White Paper on AI calls for a definition of AI with enough flexibility to accommodate technical progress while being precise enough to provide the necessary legal certainty. We support the approach that "data" and "algorithm" are the main elements of AI and that humans determine and program the goals which an AI system should attain.[2]

Ecosystem of excellence

Excellence can only be established by developing skills and capacities of all stakeholders involved. The societal challenge of regulating Artificial Intelligence systems has to be accompanied by a broad ethical discourse. An overall view is needed about the relation between the human being and AI systems shaping our societies – including all perspectives of informatics, mathematics, philosophy and ethics.
The EU should establish respective structures for such a broad interdisciplinary discourse into the existing EU structures and programmes – as effective and concrete as possible.
The framework of the new research programme Horizon Europe and the revised Coordinated Plan on AI would be possible tools for establishing a permanent socially ethical discourse accompanying the political discussion of regulating AI.

Ecosystem of trust

COMECE welcomes the approach based on new compulsory requirements limited to high-risk applications of AI. However, the scale to which this approach would be applied raises questions. The Commission suggests a risk-based approach consisting of two cumulative criteria.

a.) The AI application is employed in a sector where significant risks can be expected to occur; and
b.) the AI application is used in such a manner that significant risks are likely to arise.

We are not convinced that a sector in itself should be seen as more high-risk and other sectors should not.
To ensure full legal certainty we would suggest a system based on the examination of whether a certain AI application is used in a manner causing significant risks. In other words, for every AI application a single case analysis should be taking place.
The establishment of a risk-adapted regulatory system for the use of AI applications could be foreseen for:
> applications with some potential for harm
> applications with regular or significant potential for harm
> applications with serious potential for harm
> applications with an untenable potential for harm.

[2] White Paper on Artificial Intelligence , Scope of a future EU regulatory framework, p.16

Different consequences of regulation for each application could refer to the different level of the risk-adapted regulatory system.[3]

European Governance:

> Avoiding a fragmentation of regulating AI systems in different EU Member States it will be necessary to establish independent public coordination boards to act as a supervisory authority. Each national supervisory authority shall also carry the responsibility of regulating the governance of these technologies. They therefore have an important role to play in promoting the trust and safety of Union citizens, as well as in enabling a democratic, pluralistic and equitable society.[4]

In its contribution to the 2017 European Parliament consultation on Robotics and Artificial Intelligence, COMECE expressed perplexity on the possible creation of a new dedicated EU Agency, as robotics is an extremely sectorial domain that can be covered in broader contexts (e.g. innovation and technology); and it is important to curb excessive multiplication of Union structures. We would like to restate that in our view, the current key structures of the EU ensure sufficient support for addressing AI and robotics challenges.

We agree with the idea expressed by the Commission that fragmentation should be curbed and in this specific case a regulation would arguably be the preferable legal tool. While avoiding over-regulation, high legal certainty is to be valued and it will benefit both users and European businesses, which need to operate in a clear legislative framework to be competitive. Predictability is key, both for producers and consumers.

Should the EU opt for the establishment of some kind of coordination body devoted to AI, we would agree with the statement made in the White Paper that the *"...governance structure should guarantee maximum stakeholders participation"* and that *"Stakeholders... should be consulted on the implementation and the further development of the framework"* (page 25). We note with disappointment the absence of references to Churches, which have a specific status as partners of the EU institutions (Article 17 TFEU) and should be explicitly mentioned in this context. COMECE is obviously ready to take part in the relevant activities should this context be activated.

---

[3] See Opinion of the Data Ethics Commission Germany https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN.html;jsessionid=906153866554E1C8D819CB8F2CE00B1D.1_cid324?nn=11678512

[4] See also European Parliament ,draft report on a framework of ethical aspects of AI, robotics and related technologies https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=&reference=2020/2012(INL)

Elements on Fundamental Rights

a. Liability

Discussions on liability and AI/robotics have accelerated and deepened at a quick pace in especially in the last three years. They have shown the need for sound legal solutions, proving the necessity for adjustments to the EU legislative framework.

We warmly welcome the fact that the approach based on legal personality for robots/AI has been definitely discarded. However, possible integrations to the current EU legal framework might be necessary to make sure the solutions on liability vis-à-vis AI is effective.

Among the points which might be worth considering, we would highlight the following.

- Considering the complexity and close interconnection of different technologies in the AI context, we see the need to carefully assess whether an update is necessary for the provision that leaves up to national legislation to regulate liability of others in the supply chain, which can lead to fragmentation and incoherences.

- We would advise against any distinct liability regimes and rules based on the different extent/level of autonomous functioning of AI/robots: this option could lead to legal uncertainty due to the doubts that could easily arise in the classification of each case. In this context, we would caution against using terms like "autonomy" and "behaviour" in relation to AI, as these concepts are typical of a human person (entailing reason, choice, freedom).

- To strengthen the EU legal framework, the explicit inclusion of "software" in the definition of "product" in Article 2 of the Product Liability Directive should be considered, as this point has raised uncertainty, in particular due to the difficulty of classifications of certain softwares as products or services.

- Inclusion of clear requirements concerning transparency, as this aspect has important implications for the effectiveness of liability rules (e.g. on burden of proof). The reversal of the burden of proof, at least in certain specific cases, could prove helpful, including in link with compliance to transparency obligations.

In general, on the issue of liability, we commend the excellent study prepared by Professor Nevejans for the European Parliament Resarch Service on "European civil law rules in robotics" (2016).

b. Safety

As hinted at in the accompanying Report (pages 8-9), new provisions on *human oversight* in the context of AI self-learning products and systems should be considered with regard to Union product safety legislation. This is also in line with COMECE's emphasis on a human-centered approach to AI.

We would see merit in the Accompanying Report's suggestions at page 11 of *"Additional obligations... for manufacturers to ensure that they provide features to prevent the upload of software having an impact on safety during the lifetime of the AI products"* and of *"explicit provisions specifically requesting cooperation between the economic operators in the supply chain and the users could provide legal certainty in perhaps even more complex value chains".*

The White Paper also raises at page 14 the issue of coverage of services. The extension of General EU safety legislation, at least to high-risk services as a first step, should be assessed, so as to overcome some of the difficulties and uncertainties.

c. Algorithms

We would support a certain degree of algorithm transparency requirements, also to facilitate public scrutiny and accountability. Recommendation CM/Rec(2020)1 of the Council of Europe's Committee of Ministers to member States on the human rights impacts of algorithmic systems is to be recalled and supported[5].

d. Children

COMECE would like to highlight that the most vulnerable actor in the context of AI use and application is the child. An eventual comprehensive EU legal text concerning AI should contain strong clauses in this regard. Inspiration could, inter alia, be drawn from the provisions of the Audiovisual Media Services Directive that protect minors' physical, mental or moral development from any impairment/detriment. Provisions on dialogue with relevant stakeholders, in particular with parents and family associations, is also recommended.

In line with what is stated above, should any clause be inserted in a future EU legislative framework to have *"Explicit obligations for producers of, among others, AI humanoid robots to explicitly consider the immaterial harm their products could cause to users, in particular vulnerable users"* (accompanying Report page 8) this should cover "elderly persons in care environments" but also other key vulnerable users, such as children.

In the 2017 EP consultation on AI and robotics COMECE expressed appreciation for the work done by the Commission in supporting national authorities with regard to connected toys, in relation to the need to ensure that they guarantee full respect for the privacy and security of children. This is more generally valid and relevant for other applications that are used by children: in this context we appreciate the reference in the accompanying Report (page 5) to the risks deriving from a national case affecting children.

e. Protection of personal data

AI technologies are sophisticated and obviously need to draw on the processing of a wealth of data to be effective. However, they can also prove particularly aggressive with regard to data collection and intrusion in citizens' privacy.

---

[5] https://search.coe.int/cm/pages/result_details.aspx?ObjectId=09000016809e1154.

From our point of view, this makes requests for broad flexibility when it comes to applying the GDPR to AI difficult to justify.

With regard to the indications provided by the GDPR, we consider the principles outlined in its Article 5 GDPR as particularly relevant for the AI sector, especially the ones of lawfulness, fairness and transparency; data minimisation; integrity and confidentiality; and accountability.

A close monitoring of compliance with Art. 22 GDPR in the Member States is also particulary relevant for the AI sector. When it comes to profiling based on data concerning a person's religion, we would like to stress that the issue equally affects any believer, regardless of his/her belonging to a "majority" or "minority" and that therefore relevant considerations cannot be restricted to the latter.

Human control should remain at the center of AI use. This also plays a role in ensuring a coherent and compliant approach when it comes to upholding high data protection standards.

The European Data Protection Board's continued support to the Commission on this point will also be important.

On facial recognition technologies we would support a focus on the strict application of GDPR standards to the issue, while welcoming the possibility of exchanges and discussions on the topic. As correctly underlined by the EU Agency for Fundamental Rights (FRA) in its comprehensive paper on *Facial recognition technology: fundamental rights considerations in the context of law enforcement*[6]: *"Working with new AI-driven technologies, which are not yet fully understood and where not much experience has yet been gathered, requires the involvement of all relevant stakeholders and experts from different disciplines"*. Further EU guidance on Biometric identification systems would of course prove useful.

Fight against money-laundering

For COMECE and its member Bishops' Conferences it is important that the use of AI in view of the (desirable) fight against financial crimes - especially money laundering - does not lead to a "society of control" and to undue interference in the organisation of Churches and charitable organisations. It is crucial to balance transparency with privacy and autonomy. This is especially true in the context of an increased recourse to AI in countering these phenomena.

AI and military systems

Even though the development and use of **AI for military purposes** is excluded from the scope of the White Paper, we reiterate the call on the EU to **ban completely autonomous armed**

[6] https://fra.europa.eu/en/news/2019/facial-recognition-technology-fundamental-rights-considerations-law-enforcement.

systems without human supervision for their critical functions, and to work towards the start of **international negotiations on a legally binding instrument prohibiting lethal autonomous weapon systems**.

AI and cyber- security

The use of AI may not only bring **innovative and effective tools** enhancing security in a digital environment, but it may also open up **new vulnerabilities**. AI algorithms could be manipulated and, with the Internet of Things, lead to **faster and more destructive attacks** on **critical infrastructures**.

In the context of digital diplomacy, the **misuse of AI** can potentially have far-reaching **consequences for the democratic order**, for example, through an **uncontrolled spread of disinformation** or through **external influences** exercised by foreign state, economic or other non-state actors.

In this context, we encourage the EU, in particular, to:

- define **specific mandatory requirements** for particularly risky AI technologies **against cyber-threats** affecting public and citizens' safety
- support **capacity-building** in view of strengthening the **resilience** of **critical infrastructures**, as well as of **businesses** and **citizens** against AI-induced security challenges
- scrutinise the **role of private companies** and of the **actual beneficiaries of the effective final control** regarding the collection and analysis of personal data