

Feedback for the Commission Impact Assessment “Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence”

This is a common statement of the Augmented Law Institute of EDHEC Business School https://www.edhec.edu/en/legaledhec-research-centre#dexptabitem_2063327793 (for the list of Professors composing this group, please click on the link).

The aim of this position paper is to analyse the Inception Impact Assessment of the European Commission about a Proposal for an EU legal act regulating Artificial Intelligence. This report is based on 3 parts: 1) a definitional part, which aims to reply to the question “what to regulate?”; 2) a methodological part, which aims to reply to the question “why regulate?”; and 3) a content-based part, which aims to reply to the question “how to regulate?”.

1. Definitional part: *What to regulate?*

A first problem that we observe in the Impact Assessment and in the related White Paper is the lack of clear definitions. In particular, two terms urge to be clearly defined before to proceed:

1. artificial intelligence;
2. risk (to fundamental rights and freedoms, including human health and safety).

1.1. *The notion of AI*

- The notion of Artificial Intelligence has been already defined by the EC in a Communication of 2018, as systems that display “intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals”.¹ However, that definition has been criticized by the EC High-Level Expert Group on AI (hereinafter: AI HLEG) in a Document made public on April 2019.² In that document the HLEG proposed a new definition, which clarifies better what an “intelligent behaviour” is and what the environment analysis is: “systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s)”.
- In purely legal terms, the notion of AI is not present in any EU legal act. To the contrary, there is a notion of “software” (at Article 1(1) of the software directive³) and a notion of “automated decision-making” in the General Data Protection Regulation - hereinafter GDPR - (see Article 22). But both of these notions are potentially limited and not comprehensive enough for the phenomenon of AI.
- Both the White paper and the Inception Impact Assessment are not clear about which definition should be preferred. However, the implications can be relevant. In particular, since the definition of the

¹ Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018 COM(2018) 237 final.

² European Commission High-Level Expert Group on Artificial Intelligence, “A definition of AI: Main capabilities and disciplines”, 8 April 2019, <https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>

³ Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version)

Commission's Communication does not define what "intelligent behaviour" is, there might be problems in understanding the scope of AI notion and whether some technological systems (e.g., Covid-19 Alert Exposure Apps, automatic entrance systems, etc.) are within or outside the scope of "intelligent behaviour".

- Accordingly, what we propose is to prefer the HLEG definition, accompanied by an Annex with a non-exhaustive list of relevant examples of AI systems actually used.

1.2. *The notion of Risk*

- The notion of risk is also very problematic. Section B of the Inception Impact Assessment is largely based on the notion of risk (e.g., options 3 and 4 of the "Alternative options to the baseline scenarios"). However, it is not clear what we should mean by "risk" and how the risk should be assessed for each AI system.
- As regards the notion of risk, interpreting the White Paper and the Inception Impact Assessment (and in accordance with the GDPR (Articles 24, 25, 27, 33-35)) it seems that it is a legal notion referring to the "risk for fundamental rights and freedoms". However, such a legal notion should be based on some criteria to identify what "high" risk means. In the GDPR, high risk refers to a certain level of severity and likelihood for fundamental rights and freedoms. While in the White Paper the reference to "severity" seems to rely on the notion of "legal or similarly significant effects"⁴ (as referred to, e.g., in the GDPR, at Article 22(1) and 35(3)), in the Impact Assessment there is no mention of this severity threshold. In addition, there are no examples of high risk AI systems.
- We propose to clearly define what "risk" means and which level of *severity* and *likelihood* might amount to qualifying as "high risk". In addition, we propose to use the White Paper's definition of the severity threshold on "*legal or similarly significant effects*" to the rights and freedom of the subjects, possibly clarifying examples in an Annex where for each fundamental right or freedom mentioned in the EU Charter of Fundamental Rights there are some examples of legal or similarly significant effects. When analysing risks to fundamental rights and freedoms, particular attention should be dedicated to human health and safety. The Annex should devote specific criteria for the analysis of risk to human health and safety.

2. Methodological part: *why to regulate?*

- In the EU law there are already several different pieces of legislation covering many different areas that are generally very relevant for AI systems. Both the White Paper and the Impact Assessment do not seem to focus on existing rules. Identification and application of existing legal rules may mitigate AI-related risks and protect individuals. Accordingly, it would be helpful to understand whether there exists any gaps that the law should cover. The Inception Impact Assessment implies possible coverage and/or gaps in Products Liability Directive, but there are other rules that provide for protection against AI-related harm. A comprehensive analysis, beyond products liability, would be helpful. In this section we will make just some preliminary examples.
- Data Protection Law. The GDPR and the related data protection pieces of legislation (e-privacy directive, Law Enforcement Directive, EUDPR, PNR directive) are already requiring a certain level of accountability, transparency and fairness of AI (in particular for automated decision-making system

⁴ European Commission, White Paper on AI, p.17.

based on personal data processing). However, we identify some areas where AI systems are not based on personal data (as defined at Article 4(1) of the GDPR): as a preliminary example we can consider automated online behavioural advertisement systems in public spaces (where emotion recognition triggers different kinds of advertisements, without any need to identify the natural person, who is targeted). If these automated emotion recognition tools could in principle imply high risks for fundamental rights and freedoms of natural persons, this might be a clear example of a “gap” that a new EU legal act on AI could cover. Other examples may involve, e.g.: secondary effects of AI-driven data processing that do not affect data subjects but a bigger audience of individuals who are not clearly identified; adverse effects (e.g., anticompetitive acts) of AI on legal persons that are protectable neither under Intellectual Property Law nor under data protection law (the GDPR protects only physical persons).

- Anti-discrimination Law. EU antidiscrimination law is sectoral and category based. Accordingly, its approach, including existing burden of evidence rules, may—or may not—turn out to be highly ineffective to identify and mitigate new forms of hidden AI-driven discriminations, based on, e.g., data proxies or affinity profiling.
- Consumer Law and related Tort Law (product liability). EU protects consumers, e.g., through the limitations to unfair commercial practices and through specific protections against defective products liability. Both these areas might be relevant to protect consumers adversely affected by AI-driven commercial practices or AI-driven products. A proportionality assessment in the Impact Assessment should explain why the current legislation is (or is not) adequate to deal with AI-based practices. For what concerns the unfair commercial practice directive, it might be helpful to add in the EU blacklist of unfair practice some cases of AI-related practice that could adversely affect mental freedom of consumers. As regards product liability, we agree that clarification is needed for determining whether the directive includes software. Consistent with our proposal of a comprehensive statement regarding the effectiveness of existing law, liability for software defects should additionally be concerned with consumer protection and basic contract law principles. It may be the case the Products Liability Directive requires no amendment.
- Public Administration Law. Both the White Paper and the Inception Impact Assessment seem to refer only to AI systems developed or used by private parties (businesses), while there is no mention of possible issues or pitfalls of AI used by public institutions. The Impact Assessment should clarify why this approach was preferred and whether current administrative law (at least at Member State law level) is adequate to deal with risks to fundamental rights and freedoms for individuals generated by AI systems in public institutions (e.g., school admissions, public hospital interactions, tax anti-evasion systems, etc.).

3. Content-based part: *how to regulate?*

- The impact assessment shows several alternative options: 1) soft law; 2) voluntary labelling scheme; 3) hard law (a. based only on some categories/sectors; b. based only on high-risk AI; c. covering all AI systems); 4. a combination of the previous approached.
- In our view, in order to make this decision, it is highly necessary to reply to point 1 and 2 of this paper, i.e. clarifying the definitions and the existing gaps.

- Although each approach may have advantages and disadvantages, we consider that the voluntary labelling scheme is inefficient and ineffective for the declared purposes of a regulation on AI. Many other EU legal sectors recognize voluntary labelling scheme but *only as an ancillary tool*, related to other kinds of regulation.
- Depending on the definition of high-risk the approach 3.b might be considered, but only with a clear blacklist of high-risk examples and with easy criteria to identify risks and to correlate each risk to a fundamental right or freedom as recognized by the EU Charter of Fundamental Rights and Freedoms.
- In addition, any sectoral amendment of existing laws should be advisable (including soft law actions, as amending the unfair commercial practice blacklist, etc.).