AI

Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts

Contribution of think tank Renaissance Numérique and of the Chair on the Legal and Regulatory Implications of AI of Grenoble Alpes University

August 2021

RENAISSANCE
numerique

AI-REGULATION.COM

Table of contents

Introduction

Artificial intelligence (AI) systems bear many opportunities for the European economy and society. They also raise significant challenges for the European Union, whether in terms of its capacity to innovate – and, therefore, be competitive in this domain at the international level – or in terms of its capacity to protect European citizens from the risks these technologies may entail for their rights and liberties. When it comes to regulation, those challenges are particularly vivid. Those technologies, just like their use cases, are diverse, evolutionary, and unpredictable.

In this perspective, the European Commission led by Ursula von der Leyen has started working on ways to support the development of artificial intelligence systems in the European Union. This contribution relates to the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, presented on 21 April 2021[1].

This contribution was cowritten by think tank Renaissance Numérique and the Chair on the Legal and Regulatory Implications of AI of Grenoble Alpes University's Multidisciplinary Institute for Artificial Intelligence (MIAI). It is in line with previous contributions by the co-signatories on the European Commis-

---

1 European Commission (2021), "Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts", COM/2021/206 final, 107 pp.: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

sion's White Paper on Artificial Intelligence[2]. It also follows the co-organisation of a seminar by Renaissance Numérique, the Chair on the Legal and Regulatory Implications of AI, and Facebook, on 10 June 2021. This event gathered around forty participants involved in AI at the European level – lawyers, engineers, representatives of national and European public institutions, of civil society and companies, and researchers[3]. It aimed at questioning the relevance of the proposed regulation on artificial intelligence and its quest for a certain balance[4]. This report draws on the many ideas and opinions expressed during the seminar.

---

2 European Commission (2020), "Artificial intelligence : A European approach to excellence and trust", COM(2020) 65 final, 26 pp.: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf
See the co-signatories' contributions in the "Contributions to the consultation" section of the following page: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-requirements-for-artificial-intelligence/public-consultation_fr

3 The organisers warmly thank the participants who joined the seminar, which enabled lively and in-depth debates, in particular those who kindly accepted to share preliminary remarks to frame the discussion: Samo Zorc, Secretary, Ministry of Public Administration, Slovenia; Salvatore Scalzo, Policy and Legal Officer 'Artificial Intelligence', DG CNECT, European Commission; Maria Luisa Stasi, Senior Legal Officer, Article 19; Elise Lassus, Research Officer, 'Freedoms and Justice' Department, European Union Agency for Fundamental Rights; Marcin Detyniecki, Head of Research and Development & Group Chief Data Scientist, AXA et Vice-president, Impact AI; Kari Laumann, Head of Section for Research, Analysis and Policy and Project Manager 'Regulatory Sandbox', Datatilsynet (Norway's data protection authority).

4 In the explanatory memorandum of the proposed regulation, the European Commission mentions that: "*In light of the speed of technological change and possible challenges, the EU is committed to strive for a balanced approach.*"

I

Definitions and revision principles that raise a double concern in terms of legibility and flexibility of the regulation

As a preliminary remark, it is important to underline the progress brought about by the European Commission's proposed regulation, which ambition is to lead to the adoption of a uniform approach to the legal framework surrounding artificial intelligence systems at the European level. Indeed, given the multiple rollouts of AI systems across the European Union and the inherent issues it raises in terms of individuals' rights, developing a common legislation seemed desirable, if not necessary. The European Commission's proposal aims to foster the beneficial advances introduced by these technologies, while establishing a clear European legal framework regulating the uses of AI. The Commission's desire to implement a harmonised classification and to rely on European standards[5] seems to be a guarantee of both legibility and stability for the development of these technologies within the European internal market. The Commission's willingness to put in place a framework that is likely to have an international resonance is also worth noting, including with regard to its definition of artificial intelligence systems, which is inspired from that of the Organisation for Economic Co-operation and Development (OECD)[6].

In this perspective, two elements deserve particular attention: the legal definition of artificial intelligence systems, and the mechanisms for classifying systems as high-risk.

---

5 In this regard, see Recital 13 of the Commission's proposal.

6 The definition proposed by the OECD is the following: *"An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy."*. Source: OCDE (2019), "Recommendation of the Council on Artificial Intelligence", OECD/LEGAL/0449: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

A BROAD DEFINITION, ADAPTED TO THE REALITY AND UPGRADEABILITY OF ARTIFICIAL INTELLIGENCE?

First of all, it seems that the definition proposed by the European Commission can be qualified as utilitarian. It defines artificial intelligence systems as generating *"results"* with regard to objectives defined by humans, *"results"* that are intended to be part of the environments in which humans interact with each other and with the systems.[7]

However, the definition goes beyond this vision to qualify artificial intelligence systems. If this were not the case, it would be likely to encompass much broader technologies – than those accepted in common parlance as being artificial intelligence[8] – and for which a legal framework already exists.

The list drawn up by the European Commission – which also reserves the right to modify it[9] – enumerates in a restrictive manner the various techniques and approaches characterising an AI system[10]. As it stands, three technological approaches are being considered: machine learning approaches[11], logic- and knowledge-based approaches ("symbolic" AI)[12],

---

7 Article 3(1) of the Commission's proposal provides that "artificial intelligence system" means *"software that [...] can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;"*.

8 As an example, a simple calculator meets the characteristics of this part of the definition.

9 Article 4 of the proposed regulation provides for this possibility to amend Annex I, and article 73 sets out the terms and conditions for such amendments.

10 The limitative list of techniques and approaches that characterise an AI system is presented in Annex I of the proposed regulation: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_2&format=PDF

11 The definition of machine learning according to the Oxford Languages dictionary is the following: "*the use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyse and draw inferences from patterns in data*".

12 "Symbolic" AI was the first historical approach of artificial intelligence. This approach is essentially based on more or less explicit rules (e.g., "A implies B" or "If C and D, then E and not F") that are predefined by "expert" humans. For more information, see: https://en.wikipedia.org/wiki/Symbolic_artificial_intelligence

and statistical approaches. Based on these elements, the definition proposed in the text appears to be both broad and dynamic, which calls for two observations.

By proposing an evolving definition, which is not limited to existing techniques and approaches, the European Commission intended to propose a technology-neutral definition that is as *"future proof as possible"*, particularly in view of the rapid evolution of AI technologies[13]. However, it should be noted that the dynamism of this definition is limited to "*software*" systems, while research on other forms of artificial intelligence is currently underway[14], with the risk that the text could become less relevant if these new forms of AI were actually developed. But although adopting an approach that would broaden the definition of AI techniques beyond software systems alone would have the merit of encompassing potential future developments of these technologies, it could also create legal uncertainty[15].

Furthermore, although the text includes a procedure for revising the list of AI techniques and approaches[16], the modalities of this procedure are questionable, as the proposal grants this power of modification to the European Commission alone. Safeguards are foreseen – the European Council or Parliament can revoke the Commission's delegation of power[17] or oppose the envisaged modification[18]. However, the possibility of adopting a more open mechanism for revising the annex, involving all the stakeholders concerned for clarity and security reasons, for some of – or all – the modifications, was raised during the seminar. It might indeed be appropri-

---

13 See in this sense paragraph 5.2.1, p.12 of the proposed regulation.

14 In this regard, see, for instance: Woods, D., Doty, D., Myhrvold, C. *et al.*, "Diverse and robust molecular algorithms using reprogrammable DNA self-assembly", *Nature,* 567, 366–372 (2019): https://doi.org/10.1038/s41586-019-1014-9

15 In Recital 6, the Commission argues that a clear definition of the concept of AI system coupled with flexibility to accommodate future technological developments is necessary, p.18. This legal certainty will aim in particular to facilitate investment and innovation (p.3) within the EU, and to ensure that there are no obstacles to the cross-border movement of AI systems (p.10).

16 Article 4 of the proposed regulation provides that: *"The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend the list of techniques and approaches listed in Annex I, in order to update that list to market and technological developments on the basis of characteristics that are similar to the techniques and approaches listed therein."*.

17 Article 73(3) of the proposed regulation.

18 Article 73(5) of the proposed regulation.

ate to include all stakeholders in the revision mechanism, to ensure transparency and security.

In this regard, the role of the European Artificial Intelligence Board (EAIB) could prove central. It could be given a role as a discussion forum in which the various stakeholders could share their expertise and possibly propose amendments to the list of techniques and approaches considered as AI systems. This essential role in the elaboration of the amendments would also allow the EAIB to provide recommendations to the concerned actors in order to clarify the situation of developers or users of artificial intelligence systems *vis-à-vis* the regulation. By fulfilling this mission, the board would effectively contribute to ensuring some degree of stability and legal certainty for all actors, so that the regulation achieves its function of protecting technological advances on the one hand, and rights and freedoms on the other.

CLASSIFICATION MECHANISMS OF AI SYSTEMS: SOME CRITERIA AND EXCEPTIONS NEED CLARIFICATION

The second aspect of the proposed regulation on which the authors of this report wish to comment concerns the classification of artificial intelligence systems.

The European Commission's text provides for a pyramidal classification of AI systems based on a risk-based approach, depending on their potential use cases. While few restrictions apply to systems which use is not likely to result in significant risk[19], conversely, four use cases are expressly prohibited, and regulation is put in place for systems which use presents a high degree of risk. Although this pyramidal classification appears understandable on a theoretical level, its practical implementation may raise several difficulties.

The prohibited use cases were the subject of various comments during the seminar. Paragraphs 1(a) of article 5 of the proposed regulation prohibits *"the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm"*, while paragraph 1(b) of that same article forbids *"the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm"*. This article thus considers the potentiality of harm as a basis for prohibition. If there is no explicit derogation to these prohibitions, the criterion of the potentiality of harm as an element allowing to justify a prohibition can be questioned. Indeed, the potentiality of harm seems to be a notion

---

19 Article 52 of the proposed regulation establishes an obligation to inform individuals about systems intended to interact with natural persons, systems based on emotion recognition or biometric categorisation, and audiovisual systems that generate or manipulate content that appreciably resembles existing content.

that may prove difficult to assess[20]. The risk would be to prohibit an AI system based on a potentiality, without any damage being actually caused, thus depriving a beneficial use. Conversely, basing a ban on potential harm may lead to protecting individuals, since a system may appear not to cause any potential harm *a priori*, while its secondary or derivative uses – that were not initially anticipated – could be likely to create risks, particularly if using data that may prove biased.

A third prohibition concerns the use of social scoring systems[21] by public authorities[22]. This prohibition is not absolute, as it is limited by several factors. The first one is that a "social score" leading to unfavourable treatment is prohibited only insofar as it is carried out in a context which is different from the one in which the data was originally collected[23]. The second condition excludes unfavourable treatment that is unjustified or disproportionate to the social behaviour of natural persons or to its gravity. To ensure the full effectiveness of the principled prohibition of social scoring, these alternative conditions deserve to be clarified. Finally, the principled prohibition is only targeted at public au-

---

20 In this regard, see, for instance: Floridi, L., "The European Legislation on AI: A Brief Analysis of its Philosophical Approach", 1 June 2021: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3873273

21 In Article 5(1)c of the proposed regulation, social scoring is defined as follows: *"the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics,"*.

22 This prohibition is introduced under Article 5(1)c.

23 Article 5(1)c)i) specifies: *"detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected"*.
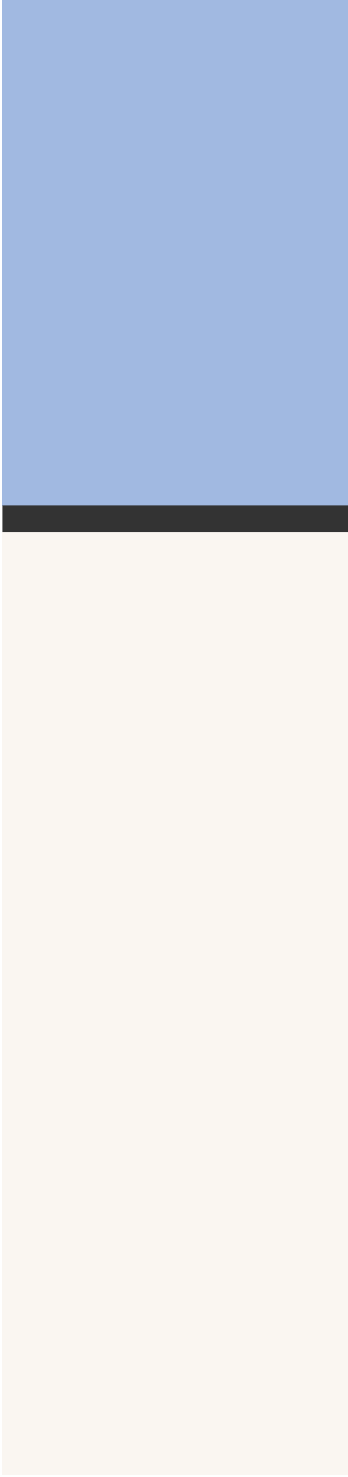
thorities. Other actors are not sub-
ject to it unless they intervene on
behalf of public authorities, even if
their uses are unjustified or dispro-
portionate, or if they take place in a
context that is different from that of
the original data collection.

Concerning the prohibi-
tion of real-time remote biomet-
ric identification systems[24], possi-
ble exceptions are foreseen by the
Commission when these systems
are used by public authorities as
part of their criminal competences.
As is the case for the above-men-
tioned prohibition, this prohibition
strictly applies to public authori-
ties for the purpose of law enforce-
ment. The use of these systems is
therefore not prohibited for other
actors, nor for public authorities,
nor for purposes other than those
related to criminal law. Moreover,
the exceptions granted for the use
of real-time biometric identifica-
tion techniques appear particularly
broad[25], which risks depriving the
prohibition of its substance. Indeed,
authorities can use such systems as
part of the prosecution of thirty-two

---

24 This principled prohibition is introduced
under Article 5(1)d.

25 The possibility to fall under these excep-
tions is conditioned to their necessity for and
proportionality to achieving the identified ob-
jective, in accordance with the requirements
of Article 10 of the Law Enforcement Directive.

criminal offences[26], but also to prevent terrorist attacks or attacks on life, or in order to locate potential victims of crimes. These three possibilities hence cover a large part of the law enforcement activities of public authorities. The reasons for including these offences in the list of exceptions (as well as for excluding other offences) should be explained in this perspective. In a recent report, the Chair on the Legal and Regulatory Implications of Artificial Intelligence has had

---

26 Those thirty-two offenses correspond to those enshrined in framework decision 2002/584/JAI: participation in a criminal organisation, terrorism, trafficking in human beings, sexual exploitation of children and child pornography, illicit trafficking in narcotic drugs and psychotropic substances, illicit trafficking in weapons, munitions and explosives, corruption, fraud, including that affecting the financial interests of the European Communities, laundering of the proceeds of crime, counterfeiting currency, including of the euro, computer-related crime, environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties, facilitation of unauthorised entry and residence, murder and grievous bodily injury, illicit trade in human organs and tissue, kidnapping, illegal restraint and hostage-taking, racism and xenophobia, organised or armed robbery, illicit trafficking in cultural goods, including antiques and works of art, swindling, racketeering and extortion, counterfeiting and piracy of products, forgery of administrative documents and trafficking therein, forgery of means of payment, illicit trafficking in hormonal substances and other growth promoters, illicit trafficking in nuclear or radioactive materials, trafficking in stolen vehicles, rape, arson, crimes within the jurisdiction of the International Criminal Court, unlawful seizure of aircraft or ships, sabotage.

the opportunity to raise several other questions related to the Commission's proposals on the regulation of biometric identification systems[27]. Finally, it should be noted that the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have issued an opinion calling for a stronger ban on these systems[28].

In addition to those prohibitions, the classification of AI systems as "high-risk" also raises questions. The concept of "high-risk", as developed in the proposal, refers both to systems that may be considered as "high-risk" because of the potential harm to the physical or vital integrity of individuals that could be caused by their use *per se*, and to systems whose malicious use would pose risks to the fundamental rights and individual and collective freedoms of people[29]. While it may seem appropriate for both types of systems to be considered as "high-risk", there are nuances between these two approaches that do not seem to have been sufficiently clarified in the proposed regulation. As these different categories of technologies entail different risks for individuals, it might seem logical to treat their marketing and assessment differently. In this perspective, some participants suggested that these nuances be taken into account in the text, in order to provide for an impact assessment that is better suited to the reality of the risks involved. This differentiation would allow actors to better identify the obligations they should respect to guarantee a sufficient level of security for systems considered to be "high-risk".

27 Christakis, T. , Becuywe, M. & AI-Regulation Team, "Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021", AI-Regulation.com, 27 May 2021 : https://ai-regulation.com/facial-recognition-in-the-draft-european-ai-regulation-final-report-on-the-high-level-workshop-held-on-april-26-2021/

28 EDPB-EDPS (2021), Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act): https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf

29 This notion of the double sense of "high-risk" was initially developed by Floridi, L., *op.* cit.

Finally, as mentioned above in relation to the revision of Annex I, some participants were in favour of a more open procedure for the revision of Annex III[30], especially from a procedural point of view[31].

Subsequently, participants questioned the robustness of the criteria that will enable the European Commission to forge a sufficient body of evidence to be likely to lead to the amendment of this annex. Two observations seem appropriate in this respect. The first one is that, for some of the participants in the seminar, there seems to be a lack of clarity around the main element for qualification. In their opinion, it is not clear, as the text is currently drafted, whether the Commission will rely on risk or on evidence of harm (or negative impact) to qualify a system as "high-risk". Clarifying this point seems necessary in order to ensure the legibility of the legal framework. The second observation concerns the margin of appreciation of certain criteria aimed at guiding the qualification of a system as high-risk. For instance, the second criterion refers to the potential uses of the system. If this criterion were to be interpreted too rigidly, there would be a risk of falsely qualifying systems which benefits may be proven. Conversely, this margin of appreciation is likely to lead to the exclusion of some high-risk AI applications from this category. This margin of appreciation, combined with the absence of a co-construction mechanism that would allow actors to anticipate legal developments, seems to create a legal framework that is too uncertain for actors involved in the development of future systems.

The lack of precision in the text regarding the possibility of extending the areas in which the uses considered to be "high-risk" fall – be-

---

30 Article 7 of the proposed regulation provides for the possibility for the Commission to add areas to the list presented in Annex III, which determines the uses qualifying as "high-risk AI systems". The first paragraph of this article sets two cumulative conditions that may lead to the amendment of Annex III: the inclusion of the proposed amendment in one of the eight existing areas of use, and the risk caused by the system at stake in terms of health, safety and fundamental rights, which should be at least equivalent to those posed by the high-risk AI systems already referred to in Annex III. The second paragraph sets out criteria for establishing a set of indicators for assessing the severity of the risk involved.

31 The amendment procedure for Annex III is also subject to the conditions laid down in Article 73 of the proposed regulation.

yond the eight areas that are already provided for[32] – can also be questioned. While this rigidity has the advantage of providing legal certainty for stakeholders, this lack of dynamism could be risky when it comes to the relevance of the text with regard to uses that may not be anticipated at the time of the initial drafting.

---

32 These eight areas which make up Annex III are the following: Biometric identification and categorisation of natural persons; Management and operation of critical infrastructure; Education and vocational training; Employment, workers management and access to self-employment; Access to and enjoyment of essential private services and public services and benefits; Law enforcement; Migration, asylum and border control management; Administration of justice and democratic processes.

"

The multi-stakeholder governance approach must be reinforced to meet the future interpretation and implementation challenges of the text

The European Commission's text aims to create a framework to foster innovation, trust, and the development of AI research and of its market within the European Union. In this respect, although the definitions and principles for the revision of AI categories are key issues[33], it is also necessary to focus on governance and on the precise role of the players who will guide the understanding but also the interpretation of this regulation. The capacity of this text to harmonise and implement the new rules relies on this governance logic.

Article 59[34] of the proposal gives Member States some latitude to designate national competent authorities tasked with, on the one hand, guiding the understanding of these rules and, on the other, ensuring that they are applied – which raises questions. It should be noted that, even though several national authorities may be competent[35], only one should be designated as the national supervisory authority or as the official point of contact within the Union[36].

While this flexibility may be welcome, a system allowing for greater harmonisation in the implementation of the regulation, to ensure an effective cooperation mechanism within the European Union, would be desirable. The Commission's AI Act proposal highlights the crucial issues

33 Many authors have written about the risk-based approach and on legal concepts which are specific to the draft European regulation. See, for instance :« Projet de règlement sur l'IA (I) : des concepts larges retenus par la Commission », *Dalloz Actualité*, Cécile Crichton, 3 May 2021 : https://www.dalloz-actualite.fr/flash/projet-de-reglement-sur-l-ia-i-des-concepts-larges-retenus-par-commission

34 In Article 59(1) of the regulation proposal specifies that national competent authorities shall be established or designated by each Member State for the purpose of ensuring the application and implementation of the regulation. Member States shall then inform the Commission of their designation or designations (including if it concerns national supervisory authorities) and, where applicable, the reasons for designating more than one authority (Article 59(3)).

35 National competent authorities may be the national supervisory authority, the notifying authority and the market surveillance authority (Article 3(43)).

36 Recital 77 of the proposal provides that *"Member States hold a key role in the application and enforcement of this Regulation. In this respect, each Member State should designate one or more national competent authorities for the purpose of supervising the application and implementation of this Regulation. In order to increase organisation efficiency on the side of Member States and to set an official point of contact vis-à-vis the public and other counterparts at Member State and Union levels, in each Member State one national authority should be designated as national supervisory authority.".*

relating to the authorisation of certain systems within the EU, such as real-time and remote biometric identification systems, which have been the subject of many questions in recent years[37].

These issues linked to the harmonisation of the implementation of European regulations are not new and have already been illustrated on several occasions, particularly following the adoption of the General Data Protection Regulation (GDPR). For instance, the creation of a new authority, the European Data Protection Board, highlighted and crystallised several fundamental questions relating to the system of governance and cooperation between Member States, but also concerning the interpretation of the text and its implementation. Questions related to the one-stop shop principle, to the cooperation between data protection authorities and to the margin of appreciation of Member States, all emerged during the adoption of the GDPR. They could arise again in the context of the regulation on artificial intelligence.

---

37 In this regard, the EDPB had first adopted guidelines on these issues as part of its "Guidelines 3/2019 on processing of personal data through video devices version 2.0" (§29) adopted on 29 January 2020 : https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf
The EDPB then clearly called for a ban of those real-time biometric identification systems following the publication of the AI Act by the European Commission, via the aforementioned joint opinion with the EDPS (see footnote 28).

In addition to the multiplicity of national authorities that could be competent, the proposal also mentions specific sectors that could and should benefit from specific provisions and designations to ensure the harmonisation of EU rules[38].

While this text raises questions as to its complementarity *vis-à-vis* other European texts, it also raises questions as to the governance mechanisms between the various supervisory authorities and actors ensuring compliance with said texts. The flexibility offered by the regulation and the margin of appreciation given to authorities raise the issue of effective European harmonisation. The effectiveness of the governance process presented in Chapter 2 of Title VI of the proposed regulation could be undermined by the latitude given to Member States both to interpret the regulation and to designate one or more competent authorities. Several governance systems indeed seem to be existing in parallel, without a clear system of communication between them. Therefore, it appears necessary to better articulate in the text how surveillance and national competent authorities will cooperate. The respective roles of the EAIB[39], Member States and the Commission should in particular be specified, especially since, in case of a disagreement, the Commission seems to have the power to decide on the withdrawal of an AI system from the market[40].

Data protection authorities (DPAs) will certainly be called upon to play a leading role in this governance. This analysis is also shared by the EDPS and EDPB. In their joint opinion of 21 June 2021[41], the two institutions call for national DPAs to be designated as supervisory authorities to en-

---

38 Recital 80 of the proposed regulation mentions that *"Union on financial services includes internal governance and risk management rules and requirements which are applicable to regulated financial institutions in the course of provision of those services, including when they make use of AI systems"* and that *"In order to ensure coherent application and enforcement of the obligations under this Regulation and relevant rules and requirements of the Union financial services legislation, the authorities responsible for the supervision and enforcement of the financial services legislation, including where applicable the European Central Bank, should be designated as competent authorities for the purpose of supervising the implementation of this Regulation, including for market surveillance activities, as regards AI systems provided or used by regulated and supervised financial institutions"*.

39 The latter is more commonly known as "the board".

40 Article 63(2) of the proposed regulation.

41 See footnote 28.

sure and contribute to a more harmonised approach. This should allow for a consistent interpretation of the provisions on data processing and avoid diverging implementation across Member States. In that sense, some participants noted that most DPAs have experience in this area and have already had to regulate and take a stance on AI systems. This vision is in line with that of the French DPA, the *Commission Nationale de l'Informatique et des Libertés* (CNIL), which, in a press release, has supported the joint opinion of the EDPB and EDPS and called for DPAs to be designated as supervisory authorities.

However, it is essential to provide these authorities with the technical and human resources necessary to take on these additional tasks. Indeed, if DPAs were to be designated as the *"supervisory authorities"* under the regulation, the text would considerably extend their scope of competence as well as their missions. While the text does provide for this[42], in practice, there are inequalities in resources and technical capacity between Member States when it comes to artificial intelligence. The low level of additional resources granted to DPAs following the adoption of the GDPR[43] highlights the risks linked to multiplying the competences granted to these authorities and the need to invest sufficiently in them within the framework of the future regulation.

No matter which authority is designated, it will be necessary to ensure that it has the capacity to take on these missions. Moreover, if DPAs are not designated as national supervisory authorities, it will be necessary to organise a consultation to ensure a coherent application of the future regulation with regard to existing regulations on data protection (GDPR, Law Enforcement Directive) within the European Union. It should however be stressed that the future regulation dedicated to AI differs from the GDPR and that the issues linked to these systems are not only related to data protection. It is also about ensuring product safety on the market and

---

42 Article 59(4) of the proposal provides that Member States shall ensure that national competent authorities are provided with adequate financial and human resources to fulfil their tasks under the regulation.

43 For an example, see: « La Quadrature du Net, Dysfonctionnements systématiques des autorités de protection des données : le cas belge », 8 July 2021 : https://www.laquadrature.net/2021/07/08/dysfonctionnements-systemiques-des-autorites-de-protection-des-donnees-le-cas-belge/

establishing a multi-actor cooperation that is not limited to collaboration between national competent or supervisory authorities but encompasses a plurality of actors[44].

Finally, the last point of analysis concerns the need to grant more autonomy to the EAIB to guarantee its independence from the European Commission. This point, which was addressed during the debate, has also been raised by the EDPS and EDPB, who question in their joint opinion the predominant role of the European Commission in this board. Indeed, the autonomy of the board can be questioned insofar as it would be chaired by the European Commission[45], which would also be responsible for convening meetings and preparing the agenda of these meetings, and for approving the board's rules of procedure[46]. This point, mentioned during the debates, questions the independence of the board and the separation of powers at the European level. These observations can be further explored through the reflections developed by Renaissance Numérique on the Digital Markets Act[47].

---

44 Data protection authorities will play a key role, but various actors such as judges, legislators and supervisory authorities will play an equally important one.

45 As defined in Article 57(3) of the proposal.

46 As defined in Article 57(2) of the proposal.

47 Renaissance Numérique (2021), "Digital Markets Act: A revolution or a legal contradiction?", 34 pp.: https://www.renaissancenumerique.org/system/attach_files/files/000/000/285/original/Renaissance_Nume%CC%81rique-NOTE_DMA_English.pdf?1617294205

III

Impact assessments: the text poses implementation challenges

Effective governance is an essential lever for the operational implementation of the new legal framework, in particular with regard to the impact assessments of AI systems required by the text. There are still many unknown variables regarding the assessment of these technologies. Given the diversity of AI systems and of their uses, determining the right scope of analysis is not always easy. An AI system is often part of analysis and evaluation processes which are larger than the AI system itself. This raises the question of the scope of evaluation, particularly in the context of impact assessments. Should the evaluation process focus on the system itself or should it consider the cross-cutting and evolving nature of the technology? The second option could, according to some participants, appear more prudent and allow for a better consideration of fundamental rights. But it could also prove less efficient, for instance by generating a mass of irrelevant data. Determining how to concretely carry out these impact assessments is thus a necessity.

In the field of artificial intelligence, certain essential principles are not yet the subject of an evaluation methodology, or even of a definitive definition. This is the case, for example, of the concept of transparency mentioned in Article 13 of the proposal[48]. It is indeed difficult to define what *"appropriate"* or *"type"* may mean in this context, or even to define the very term "*transparency*"[49].

In terms of fundamental rights, a recent study by the European Union Agency for Fundamental Rights[50], conducted among the actors of the AI value chain within the EU, has highlighted differences in the understanding of the risks AI technologies may cause to fundamental rights and in the perception of the nature of the rights that may be violated by the use of AI techniques. While the actors are particularly aware of threats related to the protection of personal data – an awareness to which the GDPR

---

48 In the first paragraph of this article, the European Commission makes an imprecise reference to *"[a]n appropriate type and degree of transparency"*.

49 To learn more, see: Renaissance Numérique (2017), « L'éthique dans l'emploi à l'ère de l'intelligence artificielle », 23 pp.: https://www.renaissancenumerique.org/publications/l-ethique-dans-l-emploi-a-l-ere-de-l-intelligence-artificielle

50 European Union Agency for Fundamental Rights (2020), "Getting the future right – Artificial intelligence and fundamental rights", 106 pp.: https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights

has undoubtedly significantly contributed – they seem much less aware of threats related to other rights, such as the principle of non-discrimination or access to remedies. In this respect, the discussions highlighted the need to strengthen the text's requirements in terms of remedies in the case of a violation of fundamental rights (or any other rights)[51].

Violations of people's rights can be assessed in the light of certain principles and values, that need to be clearly defined in advance. However, at this stage, some of the concepts presented in the proposed regulation create difficulties of interpretation. For example, Article 9 – which introduces the risk management systems required for high-risk AI systems – contains a number of terms that raise difficulties, such as *"reasonably foreseeable"* (paragraph 2(b)) or *"suitable"* (paragraph 2(d)). Article 15 is also illustrative in this respect. It refers to *"an appropriate level"* of accuracy, robustness, and cybersecurity, as well as the need for high-risk AI systems to operate in a *"consistent"* manner. Similarly, while the requirements for training, validating and testing datasets (Article 10 "*Data and data governance*") are essential, as currently drafted they raise difficulties of interpretation and implementation. Pursuant to paragraph 3 of this article, it is for instance required that these data sets be *"free of errors and complete"*. AI systems based on unsupervised learning are based on a machine learning approach that iteratively searches for patterns in large, unstructured data sets. It is therefore difficult to guarantee that these sets be free of errors.

In view of these interpretation challenges, and in line with the necessity to strengthen its role in terms of governance, the EAIB should be tasked with drawing up concrete recommendations in consultation with expert groups, relevant stakeholders, and the actors of the European artificial intelligence ecosystem. Some speakers suggested that this cooperation mechanism could be inspired by the EDPB. Support for stakeholders at the national level should also be strengthened. In addition, to bring together the diversity of expertise needed to implement the regulation –

---

51 *"The AIA could do much more to protect consumers' rights and be much more incisive about providing measures to redress the possible harms or losses that AI systems may cause. This is the part where one may expect and welcome more improvements in the proposal. It was one of the main recommendations made by the AI4People project: "7. Develop a redress process or mechanism to remedy or compensate for a wrong""*. Floridi, L., *op. cit.*

and not only expertise in terms of data protection – a "regulatory hubs" approach could be implemented. These hubs could be run by the national supervisory authorities.

To facilitate this dialogue, in addition to other information required and made public on AI systems[52], the results of impact assessments should also be made public.

---
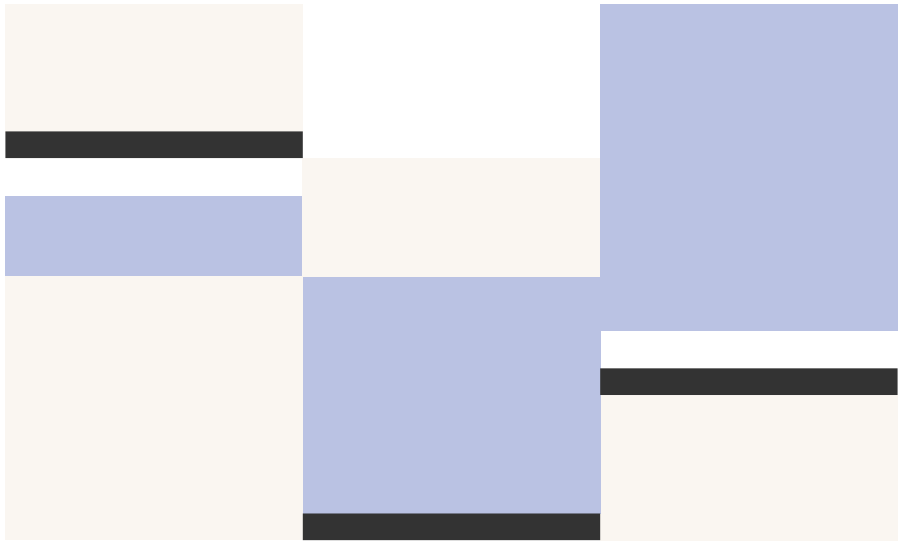
52 See, for instance, Article 60 on the EU database for stand-alone high-risk AI systems.

IV

"Regulatory sandboxes": a lever for innovation and excellence in the European Union that must be activated

In the text proposed by the European Commission, regulatory sandboxes are presented as measures aimed at supporting innovation. In that sense, they represent the "innovation" aspect of the regulatory approach of the text. The proposed regulation relies on the assumption that the existence of a stable and clear regulatory framework would enable the development of the AI market in the European Union. However, the framework remains complex and will probably not be sufficient in itself to provide an incentive mechanism likely to create a market. At this stage, the incentives included in the proposed regulation mainly concern *"small-scale providers"*[53].

It should be noted that regulatory sandboxes are also levers for co-operation between regulatory authorities, businesses, and other players in the AI ecosystem. On the one hand, these collaborations allow companies to innovate in a protective framework, since they can benefit from regulatory expertise and be quickly advised if any legal uncertainties arise. On the other hand, regulatory authorities can benefit from practical exchanges to better understand AI systems thanks to feedback from those who develop, train and deploy them, and thus possibly adapt the regulation and their recommendations accordingly. Furthermore, an effective transparency of these innovation processes could allow all stakeholders involved to create an environment of trust.

For regulatory sandboxes to work and be a real lever for innovation, it is essential to build a harmonised approach between national competent authorities, and to provide these authorities with sufficient human, technical and financial resources to implement this approach. This point is all the more crucial as national competent authorities will have an extended role: they will not only have a controlling role (ensuring the correct implementation of the regulation), but also a supporting one[54].

---

53 For instance, Article 55 "*Measures for small-scale providers and users*" provides them with compliance assistance, priority access to AI sandboxes, increased awareness tailored to their needs and a privileged communication channel.

54 This point was further developed in part 2 of this report, p. 22.

Still, this common approach could be compromised. Indeed, based on the text in its current version, *"the provisions of the regulation are not overly prescriptive and leave room for different levels of Member State action for elements that do not undermine the objectives of the initiative, in particular the internal organisation of the market surveillance system and the uptake of measures to foster innovation"*[55]. If Member States have the possibility to act freely as regards the organisation of these tools, the risk of an imbalance from one state to another is real. In this respect, the role of the board will be essential: it should *"contribute to uniform administrative practices in the Member States, including for the functioning of regulatory sandboxes referred to in Article 53"*[56].

In this perspective, the functioning of regulatory sandboxes should be discussed in a collegial manner between the European Commission, the EAIB, national competent authorities, the AI Expert Group and relevant industry and civil society representatives. For now, the functioning of regulatory sandboxes indeed varies from one Member State to another. Besides, regulatory sandboxes are most often an opportunity for DPAs to assess some compliance issues, rather than real experimental frameworks aimed to open up to innovation. Among the existing regulatory sandboxes, the competent authorities could draw inspiration from the one initiated by the British Financial Conduct Authority (FCA) in 2018 in the field of fintech[57]. This initiative stands out from others in that its ambition is global. Indeed, the British authority has created the Global Financial Innovation Network (GFIN), which brings together eleven global regulators. Its objective is to *"consider how to build new ways of sharing experience and managing emerging issues"*[58] to put an end to regulatory borders. The same logic could be followed at the European level, with the support of the EAIB. At the Union level, it would be possible to start by specific projects or by identifying priority areas.

---

55 Explanatory memorandum, paragraph 2.4.

56 Article 58(b).

57 In this regard, see on the official website of the FCA: "FCA Innovation – fintech, regtech and innovative businesses": https://www.fca.org.uk/firms/innovation

58 « La FCA rallie onze régulateurs à son idée de « bac à sable » mondial pour la fintech », *L'AGEFI*, 8 August 2018: https://www.agefi.fr/fintech/actualites/quotidien/20180808/fca-rallie-onze-regulateurs-a-idee-bac-a-sable-253655

As for the sandbox initiative launched by the Norwegian DPA, *Datatilsynet*, in 2020[59], it distinguishes itself by the transparency approach that has been put at the heart of the way it operates. The authority publishes processes and results as the sandbox progresses. This approach can prove useful not only for companies, but also for all the other players involved, who can easily access the information. As such, it could also inspire the development of future regulatory sandboxes.

---

59 See: Datatilsynet, "Sandbox for responsible artificial intelligence": https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/

Conclusion

At a time when artificial intelligence is the subject of intense competition at the international level, this new legislation should enable the European Union to set its own standards in this area. To achieve this objective, the final text will have to find a balance between innovation and the respect of individuals' rights, as put forward in its preamble[60].

Given the unpredictable nature of AI systems and the scale of their impact, such a regulation will not be implemented correctly without an agile governance – one that is open to relevant stakeholders and expertise. Just like for regulatory sandboxes, this will require the development of ambitious tools that do not oppose regulation and innovation, and which will allow the European Union to permanently establish itself as a territory of excellence and trust when it comes to artificial intelligence.

---

60 The *"balanced approach"* advocated for by the Commission in the proposed regulation aims to enable Europe to *"preserve the EU's technological leadership and to ensure that Europeans can benefit from new technologies developed and functioning according to Union values, fundamental rights and principles"*, p.1.

FURTHER READINGS

Renaissance Numérique (2020), "Facial Recognition: Embodying European values", 103 pp.: https://www.renaissancenumerique.org/system/attach_files/files/000/000/235/original/report_facial_recognition.pdf?1592553217

Renaissance Numérique (2021), "Regulation of facial recognition technologies: A comparative analysis of France and the United Kingdom", 10 pp.: https://www.renaissancenumerique.org/system/attach_files/files/000/000/291/original/RenaissanceNumerique_EventSummary_FacialRecognitionUKFR.pdf?1623223645

Theodore Christakis (2021), "Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26", 2021: https://ai-regulation.com/facial-recognition-in-the-draft-european-ai-regulation-final-report-on-the-high-level-workshop-held-on-april-26-2021/

Team AI Regulation (2021), "Facial Recognition in the Draft AI Regulation: Useful Materials": https://ai-regulation.com/facial-recognition-in-the-draft-ai-regulation-useful-materials/

CONTRIBUTIONS

*Renaissance
Numérique*

Jennyfer Chrétien, Executive Director, Renaissance Numérique

Jessica Galissaire, Studies Manager, Renaissance Numérique

Guillaume Morat, Senior Associate, Pinsent Masons

Marine Pouyat, Consultant

Annabelle Richard, Partner, Pinsent Masons

Chair on the Legal & Regulatory Implications of Artificial Intelligence

Mathias Becuywe, Research Engineer, Multidisciplinary Institute for Artificial Intelligence, Grenoble Alpes University

Stéphanie Beltran Gautron, Research Engineer, Multidisciplinary Institute for Artificial Intelligence, Grenoble Alpes University

Théodore Christakis, Professor of Law and Director of the Chair on the Legal and Regulatory Implications of AI, Multidisciplinary Institute for Artificial Intelligence, Grenoble Alpes University

Maéva El Bouchikhi, Research Engineer, Multidisciplinary Institute for Artificial Intelligence, Grenoble Alpes University

Alexandre Lodie, Research Engineer, Multidisciplinary Institute for Artificial Intelligence, Grenoble Alpes University

Anaïs Trotry, PhD Candidate, Multidisciplinary Institute for Artificial Intelligence, Grenoble Alpes University

We also warmly thank the participants who took part in the seminar of 10 June 2021.

Renaissance Numérique

Renaissance Numérique is France's main independent think tank focusing on the challenges of the digital transformation of society. Bringing together universities, associations, corporations, start-ups and schools, it aims to develop workable proposals to help public stakeholders, citizens and businesses build an inclusive e-society.

Renaissance Numérique
32 rue Alexandre Dumas - 75011 Paris
www.renaissancenumerique.org

La Chaire Legal and Regulatory Implications of Artificial Intelligence de l'Université Grenoble Alpes

The Chair on the Legal and Regulatory Implications of Artificial Intelligence has been created at the Multidisciplinary Institute in Artificial Intelligence (MIAI, University Grenoble Alpes, France). It is composed of experts in law, economics, computer and data science, all actively working in the fields of data protection, privacy, cybersecurity and AI. Its objective is to analyse the legal and regulatory questions raised by artificial intelligence and to contribute to national, European and international debates on these issues.

AI-regulation.com