Start-ups and the proposed EU AI Act

Bridges or Barriers in the path from Invention to Innovation?

by **Letizia Tomada***

Abstract: Start-ups and small-scale providers play a crucial role in our tech and innovation-driven society. The advent of artificial intelligence may represent either a driving force or an insurmountable challenge for their growth and the setup of an AI regulatory framework is decisive in determining whether small-scale providers will encounter bridges or barriers during their innovation life-cycle. In this context, this article questions whether the recent European Commission proposal for a Regulation laying down harmonised rules on artificial intelligence (AI Act) presented on 21 April 2021 would, in practice, represent a catalyst or a hindrance to the AI innovation of start-ups. It presents the challenges that AI may pose for small-scale providers and analyses selected AI provisions in light of their needs and vulnerabilities. Further, it questions to what extent the envisaged measures in support of innovation are suited to tackle the current challenges and proposes new ways to construe more bridges in the path from Invention to Innovation.

A. Introduction

1   In the context of the EU's work on the regulation of Artificial Intelligence ("AI"), on 21 April 2021 the European Commission presented its proposal for a Regulation laying down harmonised rules on artificial intelligence ("AI Act").[1] Stemming from the policy objectives enshrined in the previously published White Paper on AI[2] the current proposal adopts a 'human centric' approach and envisages a legal framework for trustworthy AI. The proposal aims at addressing the problems linked to the use of AI, without hindering its further development. While dealing with the implications for society at large, the envisaged rules and associated recitals pay attention to the needs of SMEs and start-ups.[3] The focus on this business category is noteworthy, in light of the important role that these market players have in the

---

1   European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence and amending certain union legislative acts, COM(2021) 206 final, 2021. The present analysis is based on the text presented on 21 April 2021, as it was the only proposal available at the time of writing.

2   European Commission, White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final, 2020.

3   The specific provisions will be analysed in detail in Section 6 below.

European innovation ecosystem.[4] Furthermore, the safeguard of small and early-stage businesses is all the more relevant for larger and more established ones, as they often acquire and further develop start-ups' innovations and thus can also benefit from their existence and growth. However, despite the introduction of tailored rules for small-scale providers and start-ups, it is not yet clear whether the implementation of the proposed AI Act would, in practice, represent a catalyst or a hindrance to AI innovation of start-ups. To this aim, the present contribution first provides an overview of the proposed AI Act and analyses which businesses are included in the definition of 'start-ups' and of 'small scale providers'. Further on, Section D presents the challenges that AI may pose for small scale businesses. Against this background, Section E analyses selected AI Act provisions in light of the needs of small-scale market participants and Section F questions the extent at which the envisaged measures introduced to safeguard small-scale providers' innovation are suited to address the highlighted challenges. To conclude, Section G examines the implications that the implementation of the AI Act can have on AI innovation of start-ups and proposes ways forward to address shortcomings. The scope of the analysis is limited to the implications for start-ups as providers of AI systems.

B. Overview of the AI Act and its Aims

2   AI systems are defined in Article 3(1) as "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with". Annex I contains a list of approaches and techniques for the development of AI which integrate this definition.[5] The Commission can

amend Annex I in accordance with the new market and technological developments and on the basis of characteristics that are similar to the mentioned techniques and approaches. The definition and the related list of techniques and approaches are very broad and seem to encompass a wide range of programs.[6]

3   The AI Act follows a "risk-based approach" (recital 14) with the aim to avoid risks to the health or safety or to the protection of fundamental rights of natural persons concerned (see e.g. recitals 1, 13, 27, 32, Arts. 7(1)(b), 65). The proposal distinguishes four types of risk categories. First, it prohibits the implementation and use of AI systems that present unacceptable risks. Further on, it permits the uses of both AI systems presenting high-risks and the ones with limited risks. The high-risk systems are subject to compliance with specific requirements and obligations, while the limited risk systems must comply with transparency obligations. Lastly, the proposal mentions AI systems which present only minimal risks, and which are not directly targeted in the AI Act. The present paper focuses on the development and implementation of the high-risk AI systems category and on their implications for start-ups' innovation. The specific obligations accompanying the development and implementation of high-risk systems may hinder entry of start-up AI products in the market and thus deserves particular analysis. Conversely, it is evident that AI systems causing unacceptable risks will not reach the market *by default.* The minimal-risk ones do not raise compliance issues, while the transparency requirements for limited-risk AI systems shall be respected with regard to the high-risk category. Thus, potentially related issues will be addressed in the context of that analysis. The focus on the high-risk category is also justified as many AI products may well be deemed high-risk in the future. In fact, the 'high-risk' definition encompasses AI systems that are used as a safety component of a product or products regulated by existing legislation referred to in Annex II, such as medical devices, toys, machinery or that are required to undergo a third-party conformity assessment (Article 6(1)). In addition, AI systems in Annex III are considered high-risk (Article 6(2)). Annex III contains a list of

---

4   In this regard it is important to note that between the 1940s and 1970s large companies used to contribute more than start-ups and SMEs to the innovation system, which was mainly based on economies of scale in R&D, production and distribution at large volumes. Instead, in the last two decades the innovative potential of early-stage and small firms has increased, in light of their ability to exploit commercial opportunities that arise from market changes, of the lower cost of entry and the role of venture capital and of networks where open innovation is shared. See OECD, *SMEs entrepreneurship and innovation* (Paris: OECD, 2010) 16.

5   They include not only (a) various ML approaches, but also (b) 'Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (sym-

bolic) reasoning and expert systems' as well as (c) 'Statistical approaches, Bayesian estimation, search and optimization methods'.

6   Sebastian Felix Schwemer, Letizia Tomada, and Tommaso Pasini, 'Legal AI Systems in the EU's proposed Artificial Intelligence Act' (2021) *Joint Proceedings of the Workshop on AI and Intelligent Assistance for Legal Professionals in the Digital Workplace* (LegalAIIA 2021). CEUR Workshop Proceedings, 2. http://ceur-ws.org/Vol-2888/.

eight selected areas that can be amended by the Commission (Article 7(1)) to update it according to the technological developments.[7]

4   In the context of the establishment of a regulatory framework for AI systems, the legislator emphasizes the needs of start-ups and small-scale businesses. In fact, even the explanatory memorandum to the proposal, stresses the importance of introducing provisions aimed at reducing the regulatory burden and supporting SMEs and start-ups. The stakeholder consultations prove the attention paid to their needs: 41.5% of the 352 business and industry representatives consulted were micro, small or medium-sized enterprises.[8] The explanatory memorandum highlights the need to address possible disadvantages for SMEs thereby introducing provisions to supporting their compliance and reducing their costs. Recital 72 demonstrates this intent by clarifying that the proposal foresees the establishment of regulatory sandboxes with the aim—among others—to enhance legal certainty for innovators and remove barriers for SMEs and start-ups. Both the explanatory memorandum and the recital provide a context and a basis for interpreting Title V of the AI Act, which provides for "measures in support of innovation" and in particular Article 55 envisaging the setup of measures for "small-scale providers, start-ups and users".[9]

5   Thus, the safeguard of the interests and needs of SMEs and start-ups is certainly among the objectives of the proposed regulatory framework for AI systems. Yet, to understand both the aims of the legislator and the proposal's implications, it is necessary to analyse what is meant with SMEs and start-ups and to examine in more detail the AI Act provisions relevant for this business category.

C. What are Small-scale Providers and Start-ups? Definitions, Relevance, and Characteristics

6   When referring to measures in support of innovation, both the explanatory memorandum and the

relevant recital mention the categories of 'SMEs' and 'start-ups'. Interestingly, the articles of the proposed AI Act refer instead more specifically to 'small-scale providers' and 'start-ups'. Article 3 AI Act clarifies that 'small-scale provider' means a provider that is a micro or small enterprise within the meaning of Commission Recommendation 2003/361/EC.[10] Pursuant to the Commission definition, the category of micro, small and medium-sized enterprises ("SMEs") encompass enterprises that have less than 250 employees and have an annual turnover not exceeding EUR 50 million and/or an annual balance sheet total not exceeding EUR 43 million. In particular, within the SME category, a small enterprise is defined as an enterprise with less than 50 employees and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million, while a microenterprise employs less than 10 persons and has an annual turnover and/or annual balance sheet total less than EUR 2 million.[11] From the explanatory memorandum and the recitals it is clear that the intent of the legislator is to safeguard the interests and needs of the category of SMEs as a whole. In this framework, the referral to 'small-scale providers' as limited to small and micro enterprises does not seem justified. The scope of Article 3 should therefore be broadened as to encompass the whole SMEs category.[12] Expanding the addressees would in fact result in a more ample and more efficient use of the measures in support of innovation. In addition, it is relevant to note that while the SMEs category and sub-categories are well-defined within the EU legislative framework, the same cannot be said as regards the term 'start-ups'. In fact, the AI Act does not specify which types of businesses are deemed to be included under this category. This raises the question on whether start-ups are meant to be identified always as a sub-category of SMEs or whether they refer to enterprises also above the SMEs' ceilings but with specific features and characteristics. This lack of clarity is noteworthy as it may well lead to uncertainty when deciding who is entitled to benefit from support measures.

7   In general, corporate law does not refer to 'start-ups' as a specific form of a company and often categorises the start-up enterprise under one of the more traditional types of legal entities depending

---

7   The additional AI systems that can be included shall first be intended to be used in any of the areas included in Annex III and second, they shall pose an equivalent or worse risk of harm to health and safety or to fundamental rights, than the risk posed by the systems already enumerated in Annex III.

8   Explanatory Memorandum, p. 8.

9   The provisions included in Title V AI Act are analysed in detail in Section III below.

10   Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003).

11   Article 2, Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003).

12   Therefore including companies with between 50 to 250 employees and whose annual turnover and/or annual balance sheet is between EUR 10 to 50 million.

on the type of the formal elements such as legal personality, limited liability, management, the nature of the shares and the relationships between stakeholders.[13] Yet, there is no widely accepted legal definition of a start-up.[14] In this framework, the literature has identified different categories with the aim to empirically assess the innovative activity of early-stage market entrants and, namely, 'new-technology based firms' ("NTBFs"),[15] "gazelles",[16] 'young innovative enterprises ("YIE")'.[17] However, regardless of different nomenclatures and despite the absence of a clear legal definition, it is evident that start-ups present specific features that distinguish them from established businesses and enhance their high innovative potential thereby justifying the attention to their needs and interests. Usually the start-ups' life cycle consists of a seed phase, an early-stage phase, a growth and expansion phase, and lastly a mature exit and success phase.[18] And the dynamics in which a start-up organisation operates foster a favourable environment for the development of innovation activities. First of all, within the start-up framework, the inventor does not feel a strong risk of misappro-

priation, and this encourages their innovative activity.[19] It is in fact unlikely that any investor would misappropriate the business plan invention. Secondly, during its lifecycle, the start-up organisation operates via cooperation between entrepreneurs and investors, which results in an alignment of their incentives to produce innovation. Furthermore, since the investment is usually divided in stages and the investors supporting the first round may not invest in the subsequent ones,[20] this creates a strong incentive for entrepreneurs to improve their output and innovative performance.[21] Lastly, start-ups do not have a "fear of cannibalisation", or fear of displacing already existing product lines and thus have a stronger incentive to implement new technologies.[22] Overall, these dynamics facilitate the development of innovative activities. The attention that the EU legislator gives to the safeguard of the interest and needs of small and new market entrants is therefore welcomed, in light of the relevant role these businesses play for the innovation policy. Yet, a clearer legal definition on this business category would allow to overcome uncertainty as regards rights and entitlement, and is therefore called for.

8 Along similar lines, defining the concept of innovation is not straightforward. The present analysis relies on the definition of the Oslo Manual of the OECD that refers to innovation as "a new or improved product or process (or combination thereof) that differs significantly from the unit's previous products or processes and that has been made available to potential users (product) or brought into use by the unit (process)."[23] In other words, innovation oc-

---

13   Alexandra Andhov, 'Importance of Start-up Law for Our Legal systems' in Alexandra Andhov (eds) *Start-up Law* (Edward Elgar 2020) 9, 11.

14   Ibid.

15   Defined as independently owned businesses, not older than 25 years and based on the exploitation of a technological innovation which implies substantial technological risks Arthur D. Little, 'New technology-based firms in the United Kingdom and the Federal Republic of Germany' (Report for the Anglo-German Foundation for the Study of Industrial Society 1977).

16   Defined on the sole basis of their fast growth and without the need to be young and small. Thomas Philippon and Nicolas Véron 'Financing Europe's fast movers' (Bruegel Policy Brief, No. 2008/01).

17   European Commission, "Handbook on community State Aid Rules – Including temporary State aid measures to support access to finance in the current financial and economic crisis" (2009) 14, where they are defined as small enterprises, younger than 6 years and are capable to develop technologically new or substantially improved products or processes and that have less than 250 employees and carry a high risk of commercial failure.

18   The division in phases follows the division designed in *Gerald B. Halt, John C. Donch, et al. Intellectual Property and Financing Strategies for Technology Startups* (Springer, 2017). For more details on the different organisational structures and approaches within different phases see also John Freeman and Jerome S. Engel "Models of Innovation: Startups and Mature Corporations" (2007) 50 (1) California Management Review 94, 104.

19   Ronald J. Gilson, 'Locating Innovation: The Endogeneity of Technology, Organisational Structure, and Financial Contracting' (2010) 110 Colum. L. Rev. 885, 897.

20   See William A. Sahlman, 'The Structure and Governance of Venture-Capital Organizations' (1990) 27 Journal of Financial Economics 473, 475.

21   Ronald J. Gilson, 'Locating Innovation: The Endogeneity of Technology, Organisational Structure, and Financial Contracting' (2010) 110 Colum. L. Rev. 885, 902.

22   Michael J. Meurer, 'Inventors, Entrepreneurs, and Intellectual Property Law' (2008) 45 Houston Law Review 1201, 1211.

23   OECD, OSLO MANUAL: Guidelines for collecting and interpreting innovation data, 60 (4th ed. 2018), available at <https://www.oecd.org/science/oslo-manual-2018-9789264304604-en.htm> (accessed 20.05.2020). According to Schumpeter, innovation consists of novel goods, production methods, markets, production inputs and forms of organization. See Joseph A. Schumpeter, *The Theory of Economic Development: An Inquiry into Profits, Capital, Credit, Interest, and the Business Cycle* (1934) 88-89.

curs once the invention is implemented and brought into the market. Thus, the question is whether the set-up of the envisaged AI legal framework is likely to facilitate or hinder the innovation process.

D. AI Challenges for Small-scale Businesses

9 When it comes to the challenges related to the uses of AI in organisations in general, as a starting point, it is relevant to highlight that, currently, many AI systems are only experimental and not deployed in production.[24] In fact, it may be feasible and not too cumbersome to develop and demonstrate the technical functionality of a pilot AI project. However, deployment requires a much higher variety of skills and infrastructure, such as integration with already existing technical and legal structures, reskilling of employees and changes in business processes and management.[25] And the barrier between experiment and deployment is even harder to break down for a small-scale business. The extent at which the envisaged AI Act will answer these challenges can inform the evaluation on how far it can be deemed to support innovation by small-scale providers. This Section addresses in more detail some of the main challenges that small-scale businesses face in relation to the use and deployment of AI.

I. Lack of Talent and Resources

10 Both the identification and the development of business use cases for AI systems, require a deep understanding of AI technologies, of their limitations and of their usage in the business. These tasks require a broad set of skills that encompass computer science with a focus in machine learning, robotics and physics.[26] At present, there is an AI skills gap, which can hinder the opportunities of start-ups to enter the market. And even start-ups that use already made and developed AI solutions, need skilled and trained employees able to manage and use them and to correctly interpret their results.

To overcome these skills gaps, the business entity can either train existing employees or hire and attract AI specialists.[27] Both cases, however, require considerable expenses.

II. Poor IT Infrastructure and Data Scarcity

11 Moreover, to develop machine learning and deep learning solutions with the use of AI, businesses need advanced computers and processors to solve problems at high speed. In particular, when the volume of data grows and deep learning develops even more complex algorithms, the business may well need very advanced IT infrastructure, able to process data more quickly than other computers. It goes without saying that a robust IT infrastructure, including high-performing hardware and advanced computer systems is very expensive to set-up, implement and run. In addition, even when those systems are available, start-ups need to have relevant data. And although at present, businesses have access to a greater amounts of data than ever before, it is also true that the most powerful AI machines are the ones trained on supervised training, which usually requires labelled data. Thus, a business which wants to implement AI strategies, needs to have a basic set of data and keep a source of relevant information and make sure that it can be relevant and useful for the specific industry. For a start-up this can be problematic as the data both available and relevant to it may often be very scarce.[28]

III. Detecting Bias and Privacy related Issues

12 Further on, all types of businesses when developing and deploying AI, should be aware and have to try to avoid possible dysfunctions, including risks of bias, lack of accountability or privacy issues.

13 First, the use of AI systems in prediction or classification tasks, often raises issues of bias.[29] Thus, busi-

---

24 Hind Benbya, Thomas H. Davenport, and Stella Pachidi 'Artificial Intelligence in Organizations: Current State and Future Opportunities' (2020) 19 (4) MIS Quarterly Executive 1, 5.

25 Ibid.

26 See 'Top Six Challenges Startups Face While Implementing Artificial Intelligence' (14.03.2020) available at <https://analyticsindiamag.com/top-6-challenges-startups-face-while-implementing-artificial-intelligence/> (accessed 7 May 2021).

27 Hind Benbya, Thomas H. Davenport, and Stella Pachidi 'Artificial Intelligence in Organizations: Current State and Future Opportunities' (2020) 19 (4) MIS Quarterly Executive 1, 6.

28 See 'Top Six Challenges Startups Face While Implementing Artificial Intelligence' (14.03.2020) available at <https://analyticsindiamag.com/top-6-challenges-startups-face-while-implementing-artificial-intelligence/> (accessed 7 May 2021).

29 Hind Benbya, Thomas H. Davenport, and Stella Pachidi

nesses need to perform experiments and simulations and implement debiasing techniques,[30] thereby evaluating the datasets used and involving human reviewers, with the aim to avoid and mitigate biased outcomes. Secondly, both large- and small-scale enterprises shall comply with explainability requirements. They shall be able to explain which data are used and how the model works in order to ensure trust and avoid lack of transparency.[31] Thirdly, business managers need to be also aware of accountability concerns, they should be careful of potential processes that may cause harm and should try to clarify responsibility and legal liability between the different actors interacting with the AI system upfront.[32] Fourthly, business entities need to identify and check which are the data and variables that the algorithm uses, in order to use and process data in compliance with existing regulations and to avoid any possible privacy violation.[33]

14 It can be challenging for an early-stage businesses to be aware of and adopt a strategy against the mentioned risks. To some extent, the proposed AI Act addresses these concerns and foresees related and specific requirements and obligations in particular in relation to the high-risk category.

'Artificial Intelligence in Organizations: Current State and Future Opportunities' (2020) 19 (4) MIS Quarterly Executive 1, 7. For a review of definition of bias see Xavier Ferrer, Tom van Nuenen et al. 'Bias and Discrimination in AI: a cross-disciplinary perspective' (2020) available at < https://arxiv.org/abs/2008.07309 > (accessed on 15 March 2021).

30 Daniel McDuff, Roger Cheng et al. 'Identifying Bias in AI using Simulation' (2018) available at < https://arxiv.org/abs/1810.00471 > (accessed on 13 April 2021). Supporting the use of algorithms to detect discrimination and bias see Jon Kleinberg, Jens Ludwig et al. 'Discrimination in the Age of Algorithms' (2018) 10 Journal of Legal Analysis 113 – 174.

31 Joshua A. Kroll, Joanna Huey 'Accountable Algorithms' (2016) 165 University of Pennsylvania Law Review 3-66.

32 Paul Dourish, 'Algorithms and their others: Algorithmic culture in context' (2016) 3(2) Big Data & Society, 1-11.

33 Hind Benbya, Thomas H. Davenport, and Stella Pachidi 'Artificial Intelligence in Organizations: Current State and Future Opportunities' (2020) 19 (4) MIS Quarterly Executive 1, 8; Brent Mittelstadt, 'Automation, Algorithms, and Politics: Auditing for Transparency in Content Personalization Systems' (2016) International Journal of Communication, 10, 12. For empirical evidence of start-ups' challenges related to GDPR compliance see James Bessen, Stephen Michael Impink et al., 'GDPR and the Importance of Data to AI Start-ups' available at < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3576714 > (accessed on 20 May 2021).

E. Analysis of AI Act Selected Provisions in light of Start-ups' Needs and Concerns

15 When the AI system that the start-up has implemented is deemed as high-risk, the business must ensure that it complies with the requirements included in Chapter 2 of the AI Act. The Regulation indeed sets several obligations, encompassing the establishment and maintenance of a risk management system, with the aim to identify and analyse possible current and foreseeable risks that may arise in relation to the high-risk system (Article 9). In addition, detailed requirements concern data governance, documentation and transparency, human oversight measures and accuracy and the need to follow a conformity assessment procedure. Against the backdrop of the above-mentioned start-ups' concerns, this Section provides an overview of some of the envisaged requirements, highlighting the potential challenges that their compliance may pose for small scale businesses.

I. Data and Data Governance

16 For high-risk AI systems using techniques which require the training of models, the proposed Article 10 of the AI Act establishes quality criteria for training, validation and testing data sets. Data sets must be subject to specific data governance and management practices, which, among others, concern for example, the design choices, data collection, data preparation processing operations, the examination in view of possible biases and the identification of any possible data gaps or shortcomings (Article 10(2))). Further on, datasets shall be "relevant, representative, free of errors and complete" and datasets shall take into account the specific geographical, behavioural or functional setting, considering the intended purpose for the AI (Articles 10(3) and (4)). It is evident that in order to fulfil these requirements the business must—in the first place—have access to relevant databases. Moreover, in order to setup and implement the envisaged data governance and management practices and to evaluate and analyse the specific datasets, the organisation shall possess advanced computer systems and highly specialised expertise. In particular, especially when the training datasets are large or when the models rely on large knowledge bases (e.g. Wikidata, Wikipedia, etc.), it will be extremely challenging, if not practically impossible, to verify the representativeness, completeness and correctness of the datasets.[34] If this requirement

---

34 Sebastian Felix Schwemer, Letizia Tomada, and Tommaso Pasini, 'Legal AI Systems in the EU's proposed Artificial In-

also poses great compliance challenges for large established businesses and across different domains of application, the problems are exacerbated as far as start-ups and small-scale businesses are concerned.

17 Moreover, Article 10(5) provides a legal basis for the processing of special categories of personal data for the purposes of debiasing.[35] The introduction of this provision is remarkable and should be welcomed. In fact, pursuant to Article 9 GDPR, the collection and processing of sensitive data for these purposes would have required explicitly and freely given consent.[36] This newly introduced legal basis instead, facilitates compliance with privacy and data protection requirements, thereby lowering the burden for businesses, including small scale and start-up ones.[37]

II. Documentation and Transparency

18 Providers shall also supplement the high-risk AI system with technical documentation demonstrating the compliance with relevant requirements (Article 11) and shall develop them with logging capabilities to ensure that its functioning can be traced during its lifecycle (Article 12). In addition, providers have to make sure that the AI system operates in a transparent manner and is accompanied by instructions

of use.[38] Despite the potential difficulty of drafting instructions that are 'relevant, accessible and comprehensible to users', the documentation and transparency requirements do not appear particularly burdensome and merely call for an organisational setup within the small business.

III. Human Oversight

19 Pursuant to Article 14, providers shall also design and develop the high-risk AI systems in order to guarantee proper human oversight, meaning that the AI system can be effectively overseen by natural persons while in use, with the aim to prevent or minimise potentially emerging risks to health, safety or fundamental rights. The measures aimed at ensuring human oversight shall be either identified and built into the AI system when technically feasible or identified by the provider and implemented by the user (Article 14(3)(a)(b)). The proposal provides that the measures shall allow the humans to whom the oversight is assigned, to carry out several tasks.[39] Of particular interest in this context, the accompanying recital 48 specifies that the measures guarantee that the individuals to whom human oversight has been assigned have the 'competence, training and authority to carry out that role'. As highlighted elsewhere,[40] it is interesting to note that a previous leaked draft of the proposal included a specific referral on setting up 'organisational measures' in that regard.[41] This

---

telligence Act' (2021) *Joint Proceedings of the Workshop on AI and Intelligent Assistance for Legal Professionals in the Digital Workplace* (LegalAIIA 2021). CEUR Workshop Proceedings, 6. http://ceur-ws.org/Vol-2888/

35   Art. 10(5) AI Act reads: "To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued".

36   Ibid.; Michael Veale and Reuben Binns 'Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data' (2017) 2 Big Data & Society, 2, 1–17.

37   For empirical evidence of start-ups' challenges related to GDPR compliance see James Bessen, Stephen Michael Impink et al., 'GDPR and the Importance of Data to AI Start-ups' available at <https://papers.ssrn.com/sol3/papers. cfm?abstract_id=3576714 > (accessed on 20 May 2021).

38   For a comparative overview of the main categories of information to be provided to the public, to the users and kept by providers in technical documentation, see Michael Veale, Frederik Z. Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 24 Computer Law Review International, 1, 13 (forthcoming).

39   These include the ability to fully understand the capacities and limitations of the high-risk AI system and monitor its operation, to remain aware of the tendency of automatically relying on the system output, to correctly interpret the system's output, to decide not to use the high-risk AI system in any particular situation and to intervene on its operation (Article 14(4)).

40   Sebastian Felix Schwemer, Letizia Tomada, and Tommaso Pasini, 'Legal AI Systems in the EU's proposed Artificial Intelligence Act' (2021) *Joint Proceedings of the Workshop on AI and Intelligent Assistance for Legal Professionals in the Digital Workplace* (LegalAIIA 2021). CEUR Workshop Proceedings, 7. http://ceur-ws.org/Vol-2888/.

41   The previous draft of the Article 11(3) read as follows: '3. Organisational measures as referred to in paragraph 1 shall be identified so as to ensure that the natural persons to whom human oversight is assigned by the user have the competence, expertise training and authority necessary to carry

---

is not included anymore in the current version. Interestingly, the requirement to ensure that the human has the 'authority and competence' to modify or disregard the decision, has been previously referred to as a 'social and organisational challenge' already in the context of the GDPR and of Article 29 Working Party interpretations.[42] The development and implementation of human oversight measures undoubtedly requires competence, training and authority within the organisation, which can be hard to achieve for a start-up or small scale entity. A regulatory framework encouraging the setup of measures at an organisational level to achieve those objectives would therefore be welcomed. Thus, it is suggested to reintegrate the referral to the organisational measures in the wording of the law and in particular in the context of recital 48, rather than in Article 14, so that it can be read as a mere guidance and not as a strict requirement instead. In any case, when it comes to small business entities, a mere—although concrete—referral to organisational measures may well not suffice and should instead be accompanied by the availability of concrete and external support for the setup of both the organisational and the related oversight measures.

IV. Obligations of Providers – Quality Management System, Conformity Assessment Procedure and EU Declaration of Conformity

20 Article 16 of the proposed Regulation lists several obligations of providers of high-risk AI systems which are further explained in Chapter 3. The present contribution examines in more detail only the ones that may be more relevant for start-ups and small-scale businesses to the extent that their compliance influences the entrance of the product in the market and thus, start-ups' innovation. The listed obligations require providers to ensure that the high-risk AI system is compliant with Chapter 2 requirements (Article 16 (a)), to take

action if it is not in compliance (g), to draw up the technical documentation (c), to control and keep the logs automatically generated by the AI system (d), to comply with registration obligations (f), to keep the dialogue with the relevant national competent authorities for providing information on and demonstrating the conformity with the requirements (h)(j). In particular, providers shall also set up a quality management system (b) and ensure that the AI system undergoes the relevant conformity assessment procedure and affix the CE marking accordingly (e)(i).

21 The quality management system that providers must put in place for the operation of the high-risk AI system to ensure compliance with the relevant requirements (Article 17) shall be documented and include several aspects, for example, a strategy for regulatory compliance, examination, test and validation procedures, technical specifications, systems and procedures for data management, as well as other features. The existence of a quality management system is therefore a prerequisite to be able to bring the high-risk AI system in the market. However, the setup of such a system requires a high degree of structured organisation, which start-ups may be able to achieve only through appropriate support and assistance.

22 Moreover, pursuant to Article 19, prior to going to market with a high-risk AI system, providers must ensure that the system undergoes a specific "conformity assessment procedure" in accordance with Article 43 and shall draw up an "EU declaration of conformity" in accordance with Article 49. Article 43 clarifies that there are two different types of procedure: one based on internal control and referred to in Annex VI and one based on assessment of the quality management system and of the technical documentation with the involvement of a notified body as explained in Annex VII. In particular, for high-risk AI systems listed in Annex III, point 1, where the provider has applied harmonised standards or common specifications referred to in Articles 40 and 41, they must choose either one of the two procedures.[43] When instead

---

out their role.' See also Michael Veale, Frederik Z. Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 24 Computer Law Review International, 1, 13 (forthcoming).

42 Michael Veale and Lilian Edwards 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling' (2018) 34 Computer Law & Security Review 398-404; Sebastian Felix Schwemer, Letizia Tomada, and Tommaso Pasini, 'Legal AI Systems in the EU's proposed Artificial Intelligence Act' (2021) *Joint Proceedings of the Workshop on AI and Intelligent Assistance for Legal Professionals in the Digital Workplace* (LegalAIIA 2021). CEUR Workshop Proceedings, 7. http://ceur-ws.org/Vol-2888/

43 In more detail in this regard see Michael Veale, Frederik Z. Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 24 Computer Law Review International, 1, 16 (forthcoming), highlighting how SMEs and under-represented consumer organisations and SMEs have difficulties in engaging in private standardisation processes and that it is unclear whether the currently existing efforts to include their representation would allow their meaningful participation. In fact, these stakeholders do not have experience in standardisation and may well lack proper representation. See Rob van Gestel and Hans-W Micklitz, 'European Integration through Standardization: How Judicial Review is Breaking down the Club House of Private Standardization Bodies'

the harmonised standards have been applied only in part or do not exist, the provider shall follow the procedure involving a notified body according to Annex VII. This procedure is based, first, on the assessment of quality management system by the notified body which will send the provider a notification containing the conclusions of the quality assessment and secondly, on the control of the technical documentation by the notified body which issues a technical documentation assessment certificate when in conformity with the relevant requirements. Conversely, the high-risk AI systems referred to in Annex III, points 2 to 8, must follow the procedure merely based on internal control, as indicated in Annex VI. This procedure appears to be faster as it does not involve a notified body and it poses only on the provider the burden to verify the compliance with the relevant requirements of both the quality management system and of the technical documentation. In addition, the provider must also verify that the design and development process of the AI system and the post-market monitoring is consistent with the technical documentation.

23 The proposal provides that high-risk AI systems must follow a new conformity assessment procedure when they are substantially modified and specifies that for those that continue to learn after having been placed on the market, the changes that had been predetermined by the provider shall not be regarded as a substantial modification. In addition, the conformity procedures in Annex VI and VII can be updated in light of technical developments via delegated acts. Interestingly, a derogation from conformity assessment procedure is foreseen for a limited period of time and for exceptional reasons of "public security, protection of life and health of persons, environmental protection and the protection of key industrial and infrastructural assets." It is evident that, with the exception of the cases in which derogations are allowed, both the administrative and organisational costs and the time required to undergo the conformity assessment procedure may hinder the process from ideation to deployment, and this can be particularly challenging for small scale businesses. On one hand, the envisaged Annex VII procedure appears more cumbersome as it involves the activity of a notified body and requires more steps. On the other hand, the procedure based on internal control in Annex VI seems smoother. Yet, it poses all the burden of the relevant verifications on the provider. And this requires skills and organisation that start-ups hardly possess. In addition, the burden on small-scale business providers becomes higher and more relevant considering that, pursuant to Article 48, they are required to draw up a written EU declaration of conformity for each AI system and to keep it at

_____
(2013) 50 Common Market Law Review, 179.

disposal of the national competent authorities for 10 years after the placing on the market. The EU declaration of conformity must state that the high-risk AI system at hand meets the requirements set in Chapter 2 and must contain the information indicated in Annex V, including "a statement that the EU declaration of conformity is issued under the sole responsibility of the provider" (Annex V, point 3). This means that when small-scale providers draw up the EU declaration of conformity and affix the CE marking (Article 49), they do entirely take the responsibility of declaring and monitoring the compliance with Chapter 2 requirements and related relevant obligations. This is a very challenging task that only few start-ups may be both able and willing to take up. The proposal foresees a detailed post-market monitoring and enforcement regime, which is outside of the scope of the present contribution. However, it is relevant to highlight here that non-compliance with the practices and requirements laid down in Articles 5 or 10 can be fined up to 30.000.000 EUR or up to 6% of the total worldwide annual turnover of the company. The non-compliance with any other requirement or obligation will be fined up to 20.000.000 EUR or up to 4% of the company's total annual turnover (Article 71). Although the proposal requires providers to take into account "the interests of small-scale providers and start-up and their economic viability" and calls for the effectiveness, proportionality and dissuasiveness of penalties, it must be seen how Member States will in practice take into consideration the needs of small businesses in this context and how fragmented the approaches may be. Any considerable penalty, or at times even only the risk thereof, may well cause the business to fail or even impede their access to the market. It appears essential to, first, provide them with the means to achieve compliance and secondly, foresee and implement manners to mitigate or share liability in specific circumstances.

F. The Envisaged Measures in Support of Innovation

24 In light of the challenges that the analysed provisions leave open, this Section examines the measures that the proposal envisages in support of innovation and evaluates the extent to which they may be suited to overcome challenges.

25 Among the measures in support of innovation included in Title V, the legislator envisages the setup and use of so-called 'regulatory sandboxes'. This is an example of legal experimentation, whereby "experimental law or regulation" can be defined as a legislative or regulatory instrument with limited geographic or subject-matter application and of temporary character, designed to test a

new legal solution or policy to be evaluated at the end of a defined period.[44] In particular, the term 'sandbox' in computer science refers to a testing environment where a system is monitored and prevents and impedes malicious programs from damaging a computer system.[45] In regulation instead, a regulatory sandbox is a system created to test new products and services in an artificially created regulatory environment. They allow a limited number of private firms and the supervising regulators to engage in learning, testing of novel ideas and in enabling regulatory adjustments.[46] Thus, regulatory sandboxes represent an experimental space for innovators, where they can benefit from an inapplicability or significant loosening of otherwise applicable regulation.[47] Against this backdrop, the proposed AI Act, enables the competent authorities and the European Data Protection Supervisor of Member States to establish AI regulatory sandboxes that must provide a controlled environment to allow "the development, testing and validation of innovative AI systems before their placement on the market" (Article 53(1)). The possibility to participate in a sandbox, considerably facilitates for a start-up the burden of checking compliance with the existing regulatory framework. In fact, the experiment is meant to be supervised by the competent national authorities with the aim to ensure compliance with the AI Act requirements and other relevant Union legislation. In addition, national data protection authorities or other relevant national authorities shall be "associated to the operation of the AI Regulatory sandbox" when

the innovative AI systems involve the processing of personal data (Article 53(2)). Nevertheless, the fact that the national competent authorities contribute to supervising and ensuring compliance with relevant legislation, does not impair their supervisory and corrective powers. In fact, any existing risk to health, safety and fundamental rights must be immediately mitigated or the development and testing process will be suspended (Article 53(3)).

26 Further on, the proposed AI Act attempts to overcome the concern of fragmentation of the European approach possibly resulting from the setup of national regulatory sandboxes.[48] Article 53(5) therefore provides that the competent authorities that have established regulatory sandboxes in the Member States must "coordinate their activities and cooperate within the framework of the European Artificial Intelligence Board", thereby submitting annual reports and sharing good practices, lessons learnt and recommendations. This may well help to avoid that the small-businesses concerned receive a different treatment, depending on the Member State of operation. Yet, aiming at the harmonisation of the sandboxes framework and design is necessary, but it is also of primary importance that cooperation on best practices does take into account the social and economic specificities inherent in the different national settings as well. And it may well be the role of the Board to find the optimal balance between uniformity and diversity in this context. In any case, it is clear that the legislator attempts to tackle a potential too great risk of fragmentation. The same cannot be said regarding legal certainty in this context. In fact, the proposal does not regulate in detail the design and functioning of the regulatory sandboxes. And, at the time of writing, there is actually no specific reason why further details in this regard will or should be included within the AI Act.[49] The Act provides that the modalities and conditions of the functioning of the AI regulatory sandboxes, such as the eligibility criteria, the procedure of application, the selection, the participation in and exit from the sandbox and the rights and obligations of the participants are to be established in implementing acts, adopted by the Commission in accordance with the examination procedure referred to in Article 74(2) (Article 53(6)).

44 Sofia Ranchordas, 'Experimental Regulations for AI: Sandboxes for Morals and Mores' (2021) 1 Morals and Machines, 1, 10 [forthcoming] available at < https://ssrn.com/abstract=3839744 > (accessed 20 May 2021). For more detailed literature on experimental legislation see Sofia Ranchordás, *Constitutional Sunsets and Experimental Legislation* (Edward Elgar 2014); Michiel A. Heldeweg, 'Experimental legislation concerning technological & governance innovation – an analytical approach' (2015) 3 The Theory and Practice of Legislation, 169- 193; Rob Van Gestel and Gijs V. Dijck 'Better Regulation through Experimental Legislation' (2011) 17 (3) European Public Law 539-553.

45 Katerina Yordanova, 'The Shifting Sands of Regulatory Sandboxes for AI' (KU Leuven CITIP 18 July 2019) available at < https://www.law.kuleuven.be/citip/blog/the-shifting-sands-of-regulatory-sandboxes-for-ai/> (accessed on 15 June 2021).

46 Hillary J Allen 'Regulatory Sandboxes' (2019) 87 George Washington Law Review 579-645.

47 Ross P Buckley, Arner Dougles et al., 'Building Fintech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond' (2020) 61 Washington University Journal of Law & Policy 55-98.

48 Sofia Ranchordas, 'Experimental Regulations for AI: Sandboxes for Morals and Mores' (2021) 1 Morals and Machines, 1, 20 [forthcoming] available at < https://ssrn.com/abstract=3839744 > (accessed 20 May 2021).

49 Stressing that there is no expectation for this to happen see Sofia Ranchordas, 'Experimental Regulations for AI: Sandboxes for Morals and Mores' (2021) 1 Morals and Machines, 1, 19 [forthcoming] available at < https://ssrn.com/abstract=3839744 > (accessed 20 May 2021).

27 In addition to the proper procedure and conditions of access and functioning, it is also not yet clear which is the design and the type of legal experimentation that will be adopted. In this regard, more clarification in the context of the EU legislative acts providing a legal basis for future AI regulatory sandboxes should be welcomed. In particular, a regulatory sandbox can be limited to providing guidance to the innovator (bespoke guidance) or can foresee temporary derogations and exemptions from given rules (derogations) or provide for 'regulatory comfort' about what regulators deem as compliant behaviour and their approach towards enforcement over a certain period of time (regulatory comfort-shared risk).[50] Given the wide variety of potential options and in order to guarantee uniformity at least at the level of the regulatory sandboxes' design, it should be clarified which types of experimental regimes the competent authorities of the Member States will be able to establish. In particular, it appears that a complete temporary regulatory waiver will be excluded, since Article 53(4) explicitly clarifies that the participant in the AI regulatory sandboxes "shall remain liable under applicable Union and Member States liability legislation for any harm inflicted on third parties as a result from the experimentation taking place in the sandbox." Although it is not yet clear which is the type of harm the provision refers to, namely material harm only or also harms due to a breach of rights (e.g. privacy, fundamental rights), it is evident that this provision may prove particularly problematic for a small-scale regulatory sandbox participant.

28 In this context, in order to evaluate and opt for the most suited design, it can be instructive to consider the currently existing regulatory sandboxes experiences already developed in relation to the GDPR. For example, in the United Kingdom the Beta phase of a sandbox launched by the Information Commissioner's Office is designed to foster and safeguard data protection while supporting businesses using personal data to develop innovative products and services with a proven public benefit.[51] Moreover, the Norwegian Data Protection Authority (Datatilsynet) introduced in 2020 a regulatory sandbox to guide selected companies in the development of products in

compliance with data protection law and in respect of fundamental rights.[52] During the development phase of the service or product, the sandbox prevents any enforcement measure against the companies. Yet, it does not provide a complete waiver from the Data Protection Act.[53] Along similar lines, the French Data Protection regulator (CNIL) has also introduced a regulatory sandbox that will not exempt companies from GDPR application, but will support businesses in designing and developing compliant products and services.[54]

29 Overall, the initial and currently existing legal uncertainty as for the design, modalities and conditions of the functioning of the sandbox, may result in an initial reluctance from private companies in participation. However, the adoption of subsequent EU implementing acts and the powers of the competent authorities of the Member States, leave room for the necessary flexibility and possibility of adaptation to the requirements and best practices that are deemed most appropriate in a technologically developing European legal landscape. In this framework, the establishment of regulatory sandboxes is in general of clear benefit for start-ups and small-businesses, in particular for the product development phase. Yet, at the time of writing, the absence of more detailed information concerning the design and the procedural modalities of the sandboxes' operation, do not allow to assess to what extent these will be concretely beneficial.

30 In addition, the proposal envisages specific measures tailored for small-scale providers that Member States must undertake (Article 55). Similarly, to the above discussion concerning the regulatory sandboxes, the introduction of tailored measures to support small-scale businesses shall be welcomed. Also in this context, it will be for the Board, whose tasks are referred to in Article 58, to set an appropriate balance between uniformity and diversity among the relevant practices. And only their concrete implementation can evaluate their real efficiency. Nevertheless, despite the lack of further details at the time of writing, the envisaged measures appear to provide

---

50   For more details in this regard see Sofia Ranchordas, 'Experimental Regulations for AI: Sandboxes for Morals and Mores' (2021) 1 Morals and Machines, 1, 21 [forthcoming] available at <https://ssrn.com/abstract=3839744 > (accessed 20 May 2021).

51   Six companies are currently part of the sandbox and are active in different areas, including mental health, child-centered content moderation etc). See Information Commissioner's Office, Regulatory Sandbox (2021) available at < https://ico.org.uk/for-organisations/regulatory-sandbox/ > (accessed 13 June 2021).

52   Birgitte K. Olsen,. Sandbox for Responsible Artificial Intelligence. Data Ethics. (14 December 2020) available at <https://dataethics.eu/sandbox-for-responsible-artificial-intelligence/> (accessed 13 June 2021).

53   Sofia Ranchordas, 'Experimental Regulations for AI: Sandboxes for Morals and Mores' (2021) 1 Morals and Machines, 1, 18 [forthcoming] available at <https://ssrn.com/abstract=3839744 > (accessed 20 May 2021).

54   For more details see CNIL, 'Bac à sable » données personnelles de la CNIL : appel à projets 2021' (2021) available at https://www.cnil.fr/fr/bac-a-sable-2021 (accessed 03 December 2021).

useful, but only marginal support, to small-scale businesses. In fact, on one hand, providing small-scale businesses and start-ups with priority access to the regulatory sandboxes is of great importance (Article 55 (1)(a)). While on the other hand, however, the organisation of awareness activities on the application of the AI regulation tailored to their needs and the establishment of 'channels of communication' between small-scale stakeholders—both as providers and users—and other innovators (Articles 55(1) (b) (c)) risks remaining at the level of a mere 'claim' if not accompanied by concrete support measures for the AI system operation. Similarly, a reduction of the level of fees for the conformity assessment under Article 43, proportionate to the size and market size of the small provider concerned (Article 55(2)) is helpful, but may be not sufficient for comprehensively supporting the business in undergoing the entire cumbersome procedure that will enable its product or service to reach the market.

31 In light of the above, despite the currently existing legal uncertainty and the difficulty of finding an appropriate level of fragmentation and uniformity, the introduction of measures in support of small-scale businesses and of innovation shall be welcomed. However, the result is that all the measures currently envisaged by the legislator are keen to provide great support to start-ups and small-scale businesses more during the development phase than at the deployment stage. For example, in the context of a sandbox the business participant can receive support as for the availability and use of advanced IT infrastructure, access to data and for checking compliance with existing legislation. Also, the envisaged awareness measures encourage great initiatives. Yet, these are not sufficient to support businesses at the deployment stage, i.e. for both entering and navigating the market.

G. Implications and Ways Forward

32 It is remarkable that in the context of the political ambition of a European AI development agenda, the legislator gives so much attention to the needs of small-scale businesses. Yet, considering that the envisaged measures in support of innovation are mainly limited to the 'development phase', this Section addresses solutions to overcome the existing gaps and uncertainties and highlights directions for further research. It first reviews and proposes best practices that can enhance the support at the experimental stage in the development phase. Furthermore, it promotes the adoption of additional measures and suggests amendments to the proposal that can foster and facilitate deployment for small-scale market players.

I. Development Phase

33 Some best practices that either are already in use or require further research and that can be implemented both within and outside the context of a sandbox, include tools for ongoing model improvement, for enhancing transparency and allowing the use of models with reduced data requirements. First of all, companies are currently developing tools (MLOps – machine learning operations) to monitor the models for potential inaccuracies and improve them over time.[55] When it comes to transparency and explainability, research on how to better approach those issues is still at the early-stages. There exist 'prediction explanation' tools that highlight influential variables or features, but these cannot yet be used for most complex models as the ones in deep learning neural networks.[56] In addition, research is still at early stages when it comes to new approaches to AI that can use less data. This area is relevant in light of the fact that the trend in the volume of data that many AI systems require, in particular in deep learning neural networks, may become unsustainable.[57]

34 Regarding best practices to be developed in the context of a sandbox, it is clear that a potential sandbox model cannot foresee a complete waiver from all applicable rules considering that Article 53(4) clarifies that the participants remain liable under applicable Union liability legislation for any harm to third parties resulting from the experimentation. Nevertheless, in the author's view, a sandbox regime modelled along the lines of the currently existing Norwegian 'GDPR' sandbox can be a viable solution to both ensure compliance and safeguard the interests of small-scale businesses. In fact, within this model the participant companies could find guidance in developing products and services compliant with the AI Act, data protection law and fundamental rights. And, while providing for an—at least partial—waiver from the AI Act and GDPR, the selected companies cannot be target of enforcement measures. In light of Article 53(4), the

---

55 Hind Benbya, Thomas H. Davenport, and Stella Pachidi 'Artificial Intelligence in Organizations: Current State and Future Opportunities' (2020) 19 (4) MIS Quarterly Executive 1, 9.

56 Ibid.; Royal Society 'Explainable AI: the basics' Policy Briefing (2019) 19 available at < https://royalsociety.org/-/media/policy/projects/explainable-ai/AI-and-interpretability-policy-briefing.pdf > (accessed on 11 June 2021).

57 James Wilson, Paul R. Daugherty, and Chase Davenport, 'The future of AI will be about less data, not more' (2019) Harvard Business Review available at <https://hbr.org/2019/01/the-future-of-ai-will-be-about-less-data-not-more> (accessed on 18 June 2021).

waiver can relate to aspects that do not involve the risk of causing harm to third parties. In addition, for the other relevant aspects a regime of shared risk and liability can be implemented.

35 The introduction of these practices and further research in these areas will provide support to small-businesses in complying with requirements of data governance, human oversight and will allow them to overcome the challenges concerning the lack of infrastructures and expertise.

II. Deployment phase

36 To support small-businesses in overcoming the boundaries between the development and the concrete implementation of the invention, the set-up of management and governance practices should be fostered and encouraged. Several organisations have already implemented different types of structures and roles to handle AI projects. These include appointing AI experts, creating a centre of excellence and developing an AI strategy.[58] The implementation of these or of similar practices should occur during the development phase but their maintenance and improvement during all of the business-lifecycle is key. In this regard, entities such as start-up hubs or venture capital investors may play a relevant role in supporting small-scale businesses with the set-up and maintenance of those organisational measures. The external support in the establishment of management and governance measures and the monitoring of their activities will in turn allow start-ups to implement the measures aimed at ensuring human oversight and data governance, to follow the conformity assessment procedure and to respond to the need of skills and expertise.

37 Furthermore, once the product or service has been put into the market, businesses shall keep monitoring the compliance of the AI system with all relevant requirements. As analysed above, the envisaged reduction of penalties in cases of non-compliance on the basis of the size and market-size of the business involved, is very much welcomed. However, it may well not be sufficient and small-businesses will likely keep being discouraged from

deploying their AI innovations in light of the risks of considerable penalties and liability they still may face. In this framework, it is suggested to, first, encourage mergers and acquisitions, so that the established businesses can buy out or absorb the small-business innovative activity thereby taking over all related conformity requirements and responsibilities. In a similar vein, for cases in which a complete merger is not the preferred business solution, alternative ways of cooperation with more established businesses and investors should be developed and encouraged. This would allow them to agree on regimes of shared-liability whereby the more established organisation offers concrete support to the small-business in facing the burden of the liability risk. Secondly, it is recommended to explicitly introduce a waiver, or partial waver, from liability and penalties in cases of absence of fault.[59] Such a provision would represent a 'safe-harbour' for small businesses who have adopted measures and practices to comply with all relevant requirements but might have unintentionally overlooked some compliance aspects due to their lack of appropriate resources or expertise.

38 Lastly, it is suggested to provide support to small scale providers also in the context of enforcement before national courts, for example by reducing attorney-fees or by implementing fast-track procedures. This would mitigate the risks and possible negative consequences that an action before a court would represent for small-scale businesses.

H. Conclusion

39 In conclusion, the setup of a regulatory framework for trustworthy AI may have overall positive implications for start-ups' AI innovation. In fact, the legal framework provides a safety net that helps small-scale business providers avoid becoming prey to the indiscriminate behaviour of larger incumbents. In addition, the presence of specific rules aimed at addressing and safeguarding their category is positive. However, the referral to 'small-scale providers' as limited to small and micro enterprises does not seem justified and it is therefore recommended to broaden the scope of Article 3 as to encompass the whole SMEs category. Expanding the addressees would result in a more ample and more efficient use of the measures in support of innovation. Moreover, several requirements set forth in provisions—such as those for 'human oversight', conformity assessment, and others—represent a compliance burden for small-scale providers, thereby constituting a barrier that hinders the passage from invention to in-

---

58 In this regard see the survey in Thomas H. Davenport, 'The AI advantage: How to put the artificial intelligence revolution to work' (MIT Press, 2018). For further details see Thomas Davenport and Vikram Mahidhar 'What's your cognitive strategy?' (MIT Sloan Management Review 2018) available at < https://sloanreview.mit.edu/article/whats-your-cognitive-strategy/ > (accessed on 12 June 2021); Hind Benbya, Thomas H. Davenport, and Stella Pachidi 'Artificial Intelligence in Organizations: Current State and Future Opportunities' (2020) 19 (4) MIS Quarterly Executive 1, 11.

---

59 The details and implications of such a clause will be further researched and analysed in a separate paper.

novation. Moreover, the article finds that the measures in support of small-scale providers envisaged by the legislator are mostly addressed to the development phase rather than also at the level of deployment and implementation. Thus, the envisaged measures are not sufficient to support businesses in both entering and navigating the market and their positive implications are limited.

40 In this framework, the article suggests improvements to further detail and strengthen the measures to be adopted at development level and proposes additional measures targeted at the deployment and implementation phase. These include strengthening the role of venture capital investors and start-up hubs and fostering mergers with a view to encourage the set-up of organisational and governance measures and to support small-scale businesses with their compliance-obligations. These actors shall also take into account the adoption of regimes of shared-liability. At the same time, the possibility of introducing a waiver from liability in cases of 'absence of fault' should be taken into consideration. Furthermore, support must be provided also in the event of possible actions before Courts.

41 These improvements will constitute building blocks for construing strong bridges between early-stage inventions and implemented innovation within the EU innovative ecosystem landscape.