Paris, 12 June 2020

Response to White Paper on Artificial Intelligence- A European Approach to Excellence and Trust

CEMS at HEC Paris 2019-2020

Class on Current Issues on Digital Transformation: Data Regulation, AI and Payments

David Restrepo Amariles, Associate Professor of Data Law and AI, HEC Paris
Supervisor

Jan Lukeš, Research Assistant, HEC Paris
Editor

FULL LIST OF AUTHORS

LUKEŠ, Jan
AUBERGER, Victoire
BIFERALI, Emanuele
BOUVET, Aurélia
CATTEAU, Paul
COULANGE, Emilie
D'ANGIOLO, Francesco
DEWEZ, Alexandre
DÜLKS, Julia
EL FEKIH, Laurine
FLÜCKIGER, David
FRAPECH, Jeanne
FRUCHET, Alix
GLAZIEV, Sergey
GÖKMEN, Gökçe
GUIRGUIS, Mario
JEAN-MARIUS, Marélie
KHAZANCHI, Rushap
KHURANA, Ishan
LI, Jie
NEGRI, Martino
NI CHONCHUBHAIR, Alice
NOLD, Karen
RENNER, Alexandra
RUSPANTINI, Valeria
SAVA, Beatrice
SOLEM, Nils-Fredrik
VON DOSENRODE, Benedikt
RESTREPO AMARILES, David

Disclaimer

This response was prepared by the students of the course "Current Issues on Digital Transformation: Data Regulation, AI and Payments" as part of the CEMS programme at HEC Paris. It was supervised by Prof. David Restrepo Amariles, and edited and supplemented by Jan Lukeš. The opinions and positions expressed in this response represent exclusively the views of the authors.

HEC Paris is a leading business school located in France and committed to high quality teaching and research. CEMS is an organization aiming for the international collaboration in teaching and business practice.

Preface

The importance of AI in the current world is hard to overstate. The estimated contribution of AI to the global economy is expected to grow from $2 trillion in 2018 to around $16 trillion by 2030. (1) (2) No wonder the famous computer scientist Andrew Ng called it “the new electricity”. However, while AI will indeed bring global GDP growth and open new areas of business and possibilities, it is not yet given who will benefit from this growth and under what guidelines (both ethical and legal) will AI be developed and put to use. We believe that European Union, while currently lagging behind US and China in terms of AI funding and growth, is in a position to set the trends for years to come if it succeeds in implementation of a common strategy that not only supports AI-driven GDP growth, but balances it with strong focus on AI research, ethical approach, and equal opportunity for anyone wishing to be part of the AI revolution. Such balanced approach would help the EU close the gap and become the leading force behind AI globally, thus enabling to enforce sensible and ethical regulations to ensure safety, privacy, and fairness to all its citizens and citizens of cooperating countries.

Our response to the White Paper on Artificial Intelligence contains the set of commentaries, critiques, and recommendations that we believe would help the EU achieve said balance in its AI strategy. As HEC Paris is an institution of business education and CEMS is a network dedicated to business teaching and practice, the response to the White Paper is written with that perspective in mind. We analysed the impact of several proposals on European businesses and compared it to other strategies from around the world, assessing whether the European strategy would be enough to gain the leading position by 2030 in terms of AI research and growth. We assess the feasibility of several proposals, with risks commented on and recommendations made to ensure smoother implementation. We discuss the importance of balancing regulation with more business-friendly approach that would support the SME sector, on which EU wealth is built. Finally, throughout the response we express our conviction that clarity and transparency will be essential to build trust and long-term prosperity, due to complicated and often black-box nature of AI and legislation surrounding it.

Table of Contents

EXECUTIVE SUMMARY 5

DETAILED RESPONSE 8

4. AN ECOSYSTEM OF EXCELLENCE 8

4 A. - WORKING WITH MEMBER STATES 8

4. B - FOCUSING THE EFFORTS OF THE RESEARCH AND INNOVATION COMMUNITY 11

4. C - SKILLS 15

4. D - FOCUS ON SMEs 16

4. E - PARTNERSHIP WITH THE PRIVATE SECTOR 18

4. F - PROMOTING THE ADOPTION OF AI BY THE PUBLIC SECTOR 19

4. G - SECURING ACCESS TO DATA AND COMPUTING INFRASTRUCTURES 21

4. H - INTERNATIONAL ASPECTS 22

5. AN ECOSYSTEM OF TRUST: REGULATORY FRAMEWORK FOR AI 23

5. A - PROBLEM DEFINITION 23

5. B - POSSIBLE ADJUSTMENTS TO EXISTING EU LEGISLATIVE FRAMEWORK RELATING TO AI 26

5. C - SCOPE OF A FUTURE EU REGULATORY FRAMEWORK 33

5. D -TYPES OF REQUIREMENTS 38

a) Training data 38

b) Keeping of records and data 40

c) Information provision 40

d) Robustness and Accuracy 41

e) Human oversight 41

5. E - ADDRESSEES 42

5. F - COMPLIANCE AND ENFORCEMENT 42

5. G - VOLUNTARY LABELLING FOR NO-HIGH RISK AI APPLICATIONS 43

5. H - GOVERNANCE 44

References 46

EXECUTIVE SUMMARY

In this response to the White Paper on Artificial Intelligence, published in February 2020, we comment, critique, and make recommendations to the strategy proposal of European Commission regarding the research, development, and use of AI. The response is aimed at sections 4, building an ecosystem of AI excellence in the EU, and 5, building trust through regulatory framework.

- EU-level funding in AI of €20 billion per year is proposed, however, that is equal to the current investment US makes to maintain its leadership position in AI and there exist plans to increase it. Similarly, China is currently spending similar amounts and is planning to increase the investment significantly as they openly state their plans to dominate the field of AI. No other countries intend to invest in such amounts. In general, €20 billion per year will be enough to keep the "3rd place", but not take the lead.
- Europe is fragmented in its AI research and development with no institution or company taking a clear leadership position. The creation of lighthouse centre of research, innovation and expertise would help attract talent and boost EU's research capability. However, use cases and topics of the centre research would need to be carefully selected to ensure participation of all Member States, as some topics might be less relevant to some states and research might be stalled for political reasons. One way to help mitigate such risk would be a geographically decentralized lighthouse centre, where multiple offices would have certain focuses based on regional specificity (e.g. office in Germany with focus on automotive, office in Baltics with focus on cybersecurity, etc.). Financing such institution would be a complicated issue, possibly solvable by cooperating with private sector and by using existing AI organizations or networks.
- The European Commission (EC) plans to include more AI-related topics in the education to boost the skills of future generations in this field. Here, EC should pay attention to trends in online education and should charge an organization, for example the lighthouse centre for research, with developing an online curriculum. Any educational efforts should also introduce EU's ethical values concerning AI.
- To help boost AI in SMEs, EC is planning to introduce Digital Innovations Hubs in each member state, however, the realistic need for such hub should be considered when deciding about its placement. EU should prioritize locations with large numbers of SMEs that would feasibly benefit from such Hub. Furthermore, the intended €100 million to help SMEs finance their AI transformation is absolutely insufficient in comparison with US venture capital investment and the fact that EU is more SME-focused. Lastly, EC should consider some regulatory or administrative tools be developed to help SMEs partner with larger companies, as European SMEs are often subject to an acquisition by US or Asian tech giants.

- The proposed partnerships with private sector will need to be carefully planned as European private sector, composed mostly of SMEs, might push to have fast results with immediate potential for revenue generations, which is more often not the reality in research activities. The solution could be some form of research grants awarded to such partnerships which would easy the company's need for immediate revenue. Such grants could also help finance data collection across the EU, thus emulating the ability of GAFA to compose giant data sets that allow for unique AI research.
- With the plan to introduce AI into public sector, EC should avoid being seen as "AI promoter" and make sure to prioritize "the best solution" rather than "the best AI solution" to any potential topic. In general, EC should propose a large amount of freedom to any State to pursue and implement projects of their choice and EU's role should be mainly in unification of data collection and data sharing frameworks and facilitation of knowledge sharing between public sectors of each Sate.
- EC is undertaking initiatives and programs that aim at knitting together research infrastructures and e-infrastructure resources across EU states together. These initiatives do make headway in the right direction but lack a clear roadmap and clarification of support and services to achieve the end goal of boosting infrastructure and data management capabilities across the EU in a consistent form. Additionally, EC should incentivize data owners to provide high quality FAIR data and unify access to such infrastructure and data (including access for non-EU entities).
- While the EU plans to act in 3 ways on the international AI field, however, it is difficult to assess impact of those actions as no specific outcomes were achieved and the influence of EU on guidelines published by, e.g. Google, is debatable. Furthermore, EC is not specifying any bounding enforceable treaties being, or planning to be, negotiated with actors that are unwilling to comply with European ethical guidelines, even though such actors are exactly those that EU will need to deal with in the future to ensure safety of it's citizens. While the EC's proposal to influence and participate is a good start, enforceability will be key for ensuring safe use of AI in the future.
- AI brings both pros and cons and the Commission is trying to mitigate the high risks that can threaten essential cornerstones of the EU: equality, safety, and privacy. These risks need to be addresses by regulations; however, EU should aim at creating regulations that are expected to increase the innovation incentive. Instead of designing the regulatory system beforehand, EU should facilitate dynamic and evolving regulatory framework together with innovators and private sector and minimize law lag for AI regulations. An example would be an exchange platform where regulators could be asked for their opinion on AI use cases, giving assurances and legal certainty.
- EU legislative framework will need to be altered to be better suited for AI and its applications. Here, it is recommended that a concrete mapping of responsibility be laid out in the legislation, as "who is liable?" will be an essential question in the current monocausal and anthropocentrically designed legislation. Additionally, classification of AI standalone software as a product should be considered products are bound by warranties, obligations to eliminate design defects, etc. Finally,

EU should put in place certifications and regular checks on AI systems to ensure GDPR and FAIR principles compliance, while preventing misuse of AI for purposes such as deepfake.

- The European Commission determines that the mandatory requirements of the legal framework will apply only to AI applications identified as high-risk. However, riskiness of applications is not black-or-white and such simple classification could endanger SMEs developing AI in certain industries, make EU lag behind US and China on some topics, or create a bubble of unregulated low and medium risk applications that could pose large problems in the future, despite being deemed harmless now. EC should think about expanding the riskiness classification, perhaps by adding a "medium risk" applications with partial regulation in place.
- EC acknowledges that it will be necessary to decide on the types of mandatory legal requirements to be imposed on the relevant actors. Here we stress the importance of balancing the administrative load that might discriminate SMEs from participating in high risk research. Finally, there will be need for reasonable robustness, accuracy and fairness requirements accompanied by a good compliance controller with appeal systems in place.
- It is important for regulators to check the conformity of the processes and data used to train and create the AI, however, a prior conformity assessment can be a major obstacle to innovation and a burden that may discourage the development of AI in SMEs and startups that have limited financial and human resources. EC should include a proposal on how to assist SMEs with compliance and thus being capable of competing with tech giants able to circumvent the EU regulatory framework.
- The voluntary labelling for no-high risk AI applications seems to be contradictory in nature – either it will be too much of a burden and companies won't be able to justify it, or it will be too easy to obtain and any possible advantage from doing it will be negligible.

In general, while we agree with most proposals in the White Paper, there needs to be more specificity on some topics and careful balance will need to be struck for many proposals to work. We recommend some alterations that could mitigate the implementation risks and we place high focus on topics related to SMEs. It is because they comprise the majority of EU GDP and any regulation could threaten their ability to fully utilize AI for their growth if not implemented with them in mind. Finally, we believe that Europe should speed up the changes proposed in this White Paper, as regulatory framework will need to be in place when massive growth in investments will be seen as EU will try to establish itself the leader in AI.

DETAILED RESPONSE

4. AN ECOSYSTEM OF EXCELLENCE

4 A. - WORKING WITH MEMBER STATES

Many nations and economies, including the EU, are racing to become the global leader in AI research and innovation. Therefore, a tremendous amount of money is planned to be invested in AI by the EU. For example, the European Commission is increasing the investment in AI research and innovation under the Horizon 2020 to €1.5 billion by the end of 2020 and expecting this investment to trigger an additional €2.5 billion under existing public-private partnerships over the same period (3). However, public spending is much less than that of China and the fund raised from the private sector is far behind the US as well. Therefore, it is proposed that the EU should aim for an investment of €20 billion per year, public and private sectors combined, over the following decades to push the research and development in AI.

Comparing to the US, where AI-related start-ups raised $18.5 billion from the private sector (4) and DARPA announced the 'AI Next' campaign, a multi-year investment of $2 billion to sponsor AI research and developments in universities and companies in 2019 (5), this proposed €20 billion sounds like a competitive amount to help the EU seize the AI leadership. However, this would only be true if the EU and the US are racing from the same starting line. According to a report measuring the AI progress in China, the EU and the US, released by the Centre For Data Innovation, the US is currently leading in AI in four of six metrics, talent, research, development and hardware, with China catching up closely, leading in two metrics, adoption and data, whereas the EU falls behind both, leading in none (6). Since the EU are now lagging behind the US, to replace the US and become the leader in AI, the EU needs to speed up to narrow the gap. Therefore, whether €20 billion is enough depends on where gaps exist between the US and the EU and how much is needed to fill the gaps to overtake the US.

Talents are the foundation for AI research and development. The EU had an estimated 43,064 AI researchers and 5,787 top AI researchers in 2017, ahead of the US and China (6). Combing the concerns that there is a shortage of leading AI firms in the EU and companies in the US are remarkably attracting AI talents from other nations, a consequential challenge for the EU is to retain local AI talents and attract foreign experts. Hence, there is a need for further investments to reward academic researchers and encourage AI researchers and entrepreneurs to settle in the EU. Moreover, to accommodate the increased amount of talents, there is a need for creating new positions, so further investments in building or expanding research labs and start-ups would be expected.

Venture capital and private equity funding are essential in transferring a research outcome into a business application and developing larger firms. However, it is difficult for the EU to compete against the US in AI funding because the current EU firms are typically small. 70% of private equity and venture capital investments in the EU AI start-ups in 2018 were through seed or angel rounds, while roughly 45% of investments in the US AI start-ups were made through seed or angel rounds (6). In contrast, 5% of investments in the US were at the Series C stage, while only 1% in the EU was at the Series C stage (6). The lack of large funding deals shows that AI firms in the EU are on a relatively smaller scale with a weaker ability to attract funds than those in the US. Therefore, the European Commission should escalate the budget spent on AI further to encourage fundraising from private sectors, similar to the funding strategy of Horizon 2020, so that more AI firms get the chance to sprout and grow larger.

Besides, AI systems need massive data to train the algorithm to develop an accurate model, but the cost to collect and use data in the EU is extremely high due to the lack of leading AI firms in the EU and General Data Protection Regulation. Facebook has more than 2.5 billion monthly active users as of Q4 2019 (7), which means that Facebook can collect and use the data from 2.5 billion users to train their AI programs. While none of the tech firms in the EU has this scale of data accessibility. Moreover, as enforced by GDPR, European companies are required to collect minimized data and retain data for a limited period of time, which further restricts firms' ability to explore data for novel purposes. Therefore, AI firms in the EU are pushed to spend much more than those in the US on partnering with other companies to access various datasets to develop AI solutions.

Last but not least, when AI firms are well established with their AI systems ready for implementation after a series of funding rounds, the EU also needs to invest in encouraging society to adopt AI so that the benefits of AI can be enjoyed by the whole community. According to BCG Gamma report, 32% of Chinese companies have already adopted AI into business activities and 53% are piloting AI initiatives, while the EU only has fewer than 29% companies adopt AI and fewer than 20% pilot AI (8). In this circumstance, the EU has to invest in a series of campaigns to preach the merit of AI, convey the importance of AI and demonstrate the use cases of AI. Since European residents hold a more skeptical feeling towards AI, the investment on converting social attitude in the EU would be much larger than that in the US or China.

Overall, if the US needs $20 billion in 2019 to maintain its current leading position in AI, €20 billion per year would not be enough for the EU to fill gaps mentioned above and become the leader in AI, not to mention the US would raise the investment in AI for the next decade as well.

Furthermore, the paper does not make a concrete distinction between public and private funding regarding the expected target of €20bn annually (neither does the COM(2018) 237 (3)). We think this lack of specification and lack of incentives for the member states could make complex to reach this objective. Therefore, we believe the white paper would benefit from a clarification of the respective shares of private and public funding in the target of €20 billion invested in the European Union for AI per year.

Then, when looking at the target in itself, we believe that the objective of €20 billion (almost $22 billion) is quite ambitious and could help to close the gap with USA and China in AI R&D if reached. Nevertheless, this objective seems ambitious, when looking at the €3.2 billion spent by the European union in 2016 (9).

We will now analyse the spending in AI made by the leading countries in the world, to put in perspective the announced target of €20 billion to be invested per year in the EU:

The United States still lead the race of AI capabilities. AI R&D is a top priority for the US and has enjoyed widely bipartisan support. However, when running the numbers, less than $1 billion was dedicated for non-defense AI R&D in the FY2020 budget (10). This represents only ~0.17% of the federal R&D budget (11). In addition, the DARPA, the Defense Department's research arm, has a $2 billion fund called "Next AI" to fund the most innovative projects in this domain (12). Therefore, American top position in AI R&D comes from the strength of the private sector, with more than $16.9 billion invested in 2017-2018 in AI by venture capital and private equity funds (13). Moreover, the world biggest tech companies that have been investing heavily in several AI applications, the GAFA (Google, Amazon, Facebook, Apple), come from the USA.

To this regard, EU's investment plan seems to roughly match what the United States are spending today in Artificial Intelligence. However, to be in the frontlines of AI R&D, EU should commit to give a consequent annual envelope to AI R&D but also to invest additional funds to close the current gap in terms of talents, clusters and facilities. Moreover, as it is defined as a top strategic priority for the US, the annual public and private funds dedicated to AI R&D are likely to increase greatly in the coming years, and will probably exceed €20 billion ($22 bn) per year.

Following closely behind the US in terms of AI capabilities is China. As seen before, China has a very strong governmental strategy to favor AI development. In July 2017, China released its Next Generation AI Development Plan in order to become the world leader in the field by 2030. By then, China's AI industry is expected to total RMB1 trillion (€130 billion), with AI-related fields reaching RMB 10 trillion (€1.6 trillion) (14). The latest venture capital fund created by the Chinese government is expected to invest over $30 billion in AI and related fields within state-owned firms (15). Moreover, the public funding does not come only from the national scale, but some cities also committed to invest heavily in AI. Beijing has committed $2 billion to developing an AI-focused industrial park while Tianjin, an important harbor, announced in 2018 that $16 billion will be invested in its local AI industry (16). China is really challenging the American leadership in this domain with more and more engineers, publications in the AI field, and with a very large base of mobile phone or internet users, providing the world biggest amount of data, essential for AI's development. However, some have suggested that the Chinese government was investing tens of billion dollars for AI, which appears to be exaggerated. A study unveiled provisional findings about the Chinese public spending in AI R&D, stating that the Chinese state is probably spending between $2 and $8.4 billion per year in total in AI R&D (17), even if this figure is expected to rise in the coming years. Moreover, when looking at the money invested by the private sector, China also has significant assets. The fastest growing tech companies are locating in China: Baidu, Alibaba or Tencent showed a huge interest in AI technologies to improve their services and processes (data mining, facial-recognition used as a means of payment…) (18).

As a conclusion, we can confidently say that China is taking a leap forward thanks to a government aggressive and comprehensive strategy and to tech companies at the edge of AI technologies. With €20 billion spent per year in AI, the EU plan seems comparable to what the Chinese government is currently spending. However, given the ambitious determination of China to dominate the AI R&D, we are doubting the annual allowance of €20bn will be enough to keep up with China, that will dedicate more and more money to this prioritized strategic field.

When looking at other countries quite advanced in terms of AI R&D, such as Japan or South Korea, EU's strategy seems more adequate to keep ahead of this group of "challengers".

In Japan for instance, the government released its Artificial Intelligence Technology Strategy in March 2017. This strategy includes an Industrialization Roadmap and focuses the development of AI into three phases: the "utilization and application" of AI through 2020, the public's use of AI from 2025-2030, and lastly an "ecosystem built by connecting multiplying domains", but do not precise a special amount of funding (19). The Innovation Network Corp. of Japan (INCJ), a public-private investment fund, had around $4 billion in 2018 to invest in AI-related technologies (20). In South Korea, the government recently announced its plan to spend $2 billion by 2022 to strengthen its AI R&D capacity. The plan includes the creation of six AI schools by 2020, aiming at educating over 5000 new high quality engineers to resolve the issue of the lack of AI engineers. The government also plans to fund large scale AI projects and invest to support the incubation of AI startups and businesses (20).

In comparison, the target of the European Union of investing €20 billion per year (public and private money) seems enough to close the potential gaps with these "challengers" and to keep up – or even exceed – with their AI R&D capabilities.

4. B - FOCUSING THE EFFORTS OF THE RESEARCH AND INNOVATION COMMUNITY

The European Commission's proposal is to establish a "lighthouse centre of research, innovation and expertise" that would boost the efforts of the EU to become the global centre of AI. However, even if this proposal might create synergies between EU States, we must pay attention to the very specific conditions that have to be gathered to make this solution viable in the long run.

A. A lighthouse centre of research will help the EU to catch up with leading AI actors

As mentioned in the White Paper, the objective of creating a centralized EU department dedicated to AI research is to avoid a "fragmented landscape of centres of competences with none reaching the scale necessary to compete with the leading institutes globally". Reaching such a goal has become crucial for Europe as scale is a prerequisite when it comes to AI research. Indeed, this cutting-edge technology is very costly (e.g. expensive data collection process, advanced infrastructures with high computing capacities, salaries of top AI researchers up to €300,000 per year according to Forbes etc.) so significant economies of scale would be generated by gathering the EU forces around a common institution. In addition to these benefits related to scale, a lighthouse centre of research would be extremely powerful to attract talents. Indeed, just like the successful model of technopoles (IT clusters) have contributed to stimulate the research ecosystem in European regions in the last 40 years, a 5 centralized AI institution would boost the research environment by facilitating knowledge transfers between the key AI stakeholders all gathered in a common area (researchers, universities, tech companies etc.). Thus, a lighthouse centre of innovation is crucial to stop the brain drain phenomenon from Europe towards regions more advanced in the AI sector, such as China (strong investment strategy of 130 billion euros in AI by 2030), the GAFA (with 3.9 billion dollars invested only for Google since 1998), or even Israel which has for instance more tech companies than Germany and France put together (study about *Global Artificial Intelligence Landscape* done by Roland Berger and Asgard in 2018). As a result, the development of a centralized institution fully dedicated to AI research is the only way for Europe to quickly catch up with the main AI actors in the world.

B. But its implementation will require a greater level of cooperation between States, which might be hard to manage

Even if in theory the principle of gathering the EU research about AI in a single "lighthouse centre" (instead of having many smaller structures across Europe) sounds very promising, its implementation appears much more difficult. First, there is a risk of polarization: this centralized institution would be located in a specific country in Europe, so the risk is to have one Member State more involved than the other ones. This host country could for instance see people with its nationality more represented than others among AI searchers, or benefit more from the new infrastructures created (5G network, Universities, transportation system etc.). Then, although the initial goal of having a centralized and common infrastructure is to make all EU countries work together towards the same direction, it might lead to the opposite effect: some countries might not feel any direct impact and then become discouraged to cooperate. We can mention this threat based on the example of the Common Agricultural Policy (CAP) which is strongly criticized by some EU States (e.g. Denmark) as an "unfair measure" that does not have the same positive impact on every country. Then, the risk is to see the emergence of a Multi-Speed Europe with a limited number of countries involved in AI research, whereas others would reduce their efforts in this domain. Another source of concern is about the transfer of information that might be complex between countries. Indeed, as mentioned in the White Paper, the lighthouse centre would focus on key sectors such as “industry, health, transport, finance, agrifood value chains, energy/environment, forestry, earth observation and space” (paragraph 4.B). However, today several of these sectors are managed by each EU country at a national level. Thus, before developing common AI solutions for these sectors, the 1st required step might be to cooperate in these fields to clearly identify use cases for AI technology. For instance, the starting point of a cooperative work about AI could be the space sector as knowledge is already shared at a European level thanks to the intergovernmental European Spatial Agency (ESA) founded in 1975. As a result, an EU lighthouse centre for AI research can only be viable in the long term if Member States make sure to develop more cooperation in many different sectors.

C. Spreading testing centres across Europe based on national specificities would help build a feeling of belonging to an AI European Community

In addition to the creation of a lighthouse centre dedicated to AI research, the White Paper promotes the development of testing and experimentation sites: “the Commission will facilitate the creation of excellence and testing centres that can combine European, national and private investments.” (Action 2, paragraph 4.B). Once the exploration phase has been developed by the centralized lighthouse centre, sharing the experimentation phase across different sites would be crucial to make sure to involve as many EU countries as possible (avoiding the polarization threat mentioned above). Thus, the goal would be to define the location of testing sites based on national strengths: sites dedicated to autonomous vehicles could for instance take place in Germany (e.g. the Cyber Valley in the state of Baden-Württemberg has developed key partnerships between AI searchers and actors of the car industry), or in Sweden for robotics (e.g. the last survey launched by the European Commission concerning Automation in daily life showed that 80% of Swedes have a positive opinion about robots, Vs only 61% for the EU average). The point here is to insist on the importance of national specificities. Indeed, building an ecosystem of excellence can only be successful if many EU countries take part in this common project: spreading testing centres in several European countries would help strengthen a feeling of belonging, so crucial in the history of the European construction.

Evidence suggests that establishing a centralized research facility for AI would be very beneficial for the European Union to ensure a leadership position in the international landscape. In fact, even though Europe is currently in a good situation when it comes to the quality of its research with 30% of the top publications on AI originating from the European continent, it is very important to guarantee the maximum level of collaboration among different countries to avoid being overwhelmed by the US which can count on higher support from private investors, or by China which already has a strong centralized system and it is far head on the technology on Facial Recognition (21).

However, establishing such an institution will not be an easy task if the current European situation is taken into consideration. In fact, most European countries already have their own research facility which focuses on specific topics and it adopts its own funding methodology. For example, in Germany the German Research Centre for Artificial Intelligence (DFKI) is an established non-profit organization founded in 1988 with three different research offices on German soil and it specializes in application for the health, retail and production industries (22). Or even in Italy there is the presence of a 30-year-old research centre called FBK-ICT which specializes on human interaction AI and in System oriented AI (23). And generally, there are even several research centres within the border of the same country. For these reasons it will not be easy to create a central facility to coordinate the efforts and the investments of already existing institutions.

Another important obstacle that must be overcome in order to create this "lighthouse centre of research" in the near future, is its costs, which will comprehend the costs of salaries of researchers and other costs related to setting up such an international institution. Furthermore, several members of the European Parliament are already sceptical regarding this initiative since the budget for 2021-2027 is already constrained and there are other topics that are in need of more funding like the plan of making Europe the first climate neutral continent by commission executive vice president Frans Timmermans (24). To overcome this obstacle, it would be important to gather as much as possible funding from the private sector, for example by offering fiscal benefits or other kind of advantages to firms that would decide to invest in this European institution.

To create an institution such as the one that is proposed in the White Paper, the EU could try to model it over past successful experiences similar to this, like for example the CERN. In fact, when at the end of the second world war European research on science was struggling behind the superiority of American and soviet scientists, the CERN laboratory was created as a way to unite the different efforts made on science by European nations (25). CERN is a prime example of how research can foster collaboration among countries and can transfer its benefits towards universities and private companies. A future "lighthouse centre of research" could try to replicate the structure of an institution such as CERN even though some differences are required. For example, CERN is mainly funded by its member and observing states, while in the case of a European research centre for AI, at least at the beginning, the funding should be gathered partly from the European Union itself and from the private sector, in fact it would be impossible to compete against the US or China without a strong support from the private sector. Another difference that should be taken into Account between the CERN laboratory and this initiative is the fact that CERN occupies a very central role in the scientific research counting almost 2500 employees, while on the other hand this "lighthouse" should have more the role of creating coordination and networks among existing national research centres for AI, and maybe only in the long term it could aspire to become a central institution such as CERN.

In the creation of this research centre it would be important to consider the acquisition of talent without which it will not be possible to be competitive against international actors. In this aspect, even though

Europe can count on its strong academic ecosystem which generates talented researchers it would be imperative to come up with the right solutions to attract them towards this "lighthouse centre for research". This is a particularly difficult task if we consider what salaries the international tech companies are offering. In order to solve this issue, the European Union should try to offer salaries in line with those of the competition and it should try to co-operate directly with universities to acquire these talents as soon as possible.

Another way of setting up a central research for AI in Europe would be to direct more resources to already present networks for the research on AI. For example, in 2018, several research institutions located around Europe had already organized themselves in an organization to promote "AI made in EU" called CLAIRE. This organization can already count on an extensive network and has already the support of nine different countries (26). Another organization that is already present in Europe is ELLIS, which was also founded in 2018 by most advanced researchers in Machine Learning in Europe and want to create a network of students and experts to promote European research (27).

4. C - SKILLS

Today, Europe is facing an acute shortage of digital skills: almost half of European companies lack cybersecurity, artificial intelligence, and robotic skills (28). The EU AI plan is intending to "increase awareness of AI at all levels of education", but what levels are they referring to exactly? From what age should European citizens be exposed to digital learning?

Knowing how critical and strategic it will be in the future for the continent, would it make sense if students were learning it from a very young age, becoming a school subject on its own? It is well-known that the younger you are, the easier it is to learn a language. Then why not do the same for coding? For example, several countries including Australia, Finland, Italy and England have developed coding curriculum for children between the age of five and sixteen (29). However, children learning code is controversial: according to the OECD Education Chief, "teaching children coding is a waste of time" as the skill may become obsolete by the time they become adults (30), which is a risk that would need to be reflected in the curriculum.

The Paper also states that "particular efforts should be undertaken to increase the number of women trained and employed in this area." Indeed, 22% of AI professionals globally are female, compared to 78% who are male (31). This trend is also valid in Europe. But how can you close such a gender gap? Europe has to do extensive work in getting young girls excited for coding and innovation at an early age. In this sense, it supports the previous point as it could be useful to introduce Artificial Intelligence as early as high school or before, so that young women have an easier chance of trying it and may consider it as a career.

Furthermore, the digital age questions and reshapes our worldwide traditional secondary education system and this change was even more accelerated by the Covid-19 pandemic. Can the future skilled workers in AI come from other fields of study? This is more and more being questioned as developers can learn skills by themselves through online classes and Open Source material. Some universities understood this and started developing their AI / Data Science Online Programs such as NYU Stern business school (32). It is strategically important for European educational institutions to be part of this Online Learning trend as soon as possible.

In recent years, traditional educational institutions are facing a new competition from new digital players and big Tech players, such as the GAFA. For example, Google is increasing its presence in Online Learning: “Google has a vision to make world-class developer education accessible to students and developers”. There is also a “Google Developers Certification” that you can obtain after taking an exam (33). Will a Google Certification Degree have more credit than a Top-tier Business School diploma in a few decades? One solution for institutions and for the Lighthouse Centre of Research could be to partner with these GAFA and other tech players and to consider them as true partners in education, while keeping a preference for European players.

Lastly, the White Paper states that there should be some “ethical guidelines” indicatives for the curriculum of member states. It is indeed necessary to have some common ground rules among the states. These ethical guidelines are the occasion to reinforce European values. This trend towards ethical AI is happening worldwide: in 2019, Chinese scientists and engineers have released a code of ethics for artificial intelligence, showing that the whole world is concerned about the right use of this technology (34).

4. D - FOCUS ON SMEs

The White Paper aims to increase competitiveness of European companies in the data economy and Artificial Intelligence. However, as stated in the response to section 4A., the European Union lags behind other parts of the world like the United States and China in terms of investment in research and innovation to compete with international companies.

Small and medium enterprises, although less visible than large corporations in the field of innovation and in the economy in general, contribute to more than half of the economic value in the European Union (35). SMEs, especially startups, are typically more agile and prone to innovation (36). However, SMEs do not have the same funding capabilities as large corporations to invest in Artificial Intelligence. Indeed, AI requires large amounts of data and powerful computing infrastructure to analyse it and run algorithms. Therefore, there is a need at the European Union level to create financing tools specifically for these smaller companies.

The European Commission suggests several tools to ensure access to AI to SMEs. Some tools, like the Digital Innovation Hubs and the platform for AI “AI4EU”, are pre-existing and the White Paper mentions that Commission aims at using them to further facilitate access of SMEs to AI, as well as creating an ecosystem in which SMEs can be in relation to each other to foster synergies in investments and innovation. Some other tools, however, need to be defined and elaborated in partnership with EU member states as they are not yet in full operational condition.

A. Digital Innovation Hubs

The European Commission aims to have one Digital Innovation Hub in each region as part of the Horizon 2020 plan (37). However, this objective does not take into account the geography and concentration of innovative SMEs in clusters that make it easier for technological and business synergies to emerge in AI ecosystems: the hubs should be where there is a need from companies and not just automatically everywhere in Europe, where funding would be ineffective.

B. AI-on-demand platform

The project of the AI4EU platform was launched in 2019 with the aim to provide a one-stop ecosystem for all actors in the AI sector, from academics to entrepreneurs, to share AI tools However, this platform is too large and vague, stretching from funding to education through research. It is not clear how it can be used by SMEs as it is still in its Beta version. Although it will probably provide useful AI resources, it appears to be too general to be a real help for SMEs to access AI when they do not already have knowledge and technological capabilities.

C. European Investment fund in AI and blockchain

The European Commission has announced an investment fund of initially €100 million to help SMEs finance their AI transformation. However, this figure is to be put in perspective with other countries. In the US for instance, investment in AI from Venture Capital funds amounted to US$8 billion in 2018 alone (38). In its aim to overcome the US in AI rankings, the Chinese government plans to invest tens of billions of USD for Artificial Intelligence (38). The AI investment in the EU therefore looks limited and disproportionate, especially when taking into consideration that more than half of the economic value in the European Union is created by SMEs (35).

D. InvestEU

One key element for enabling small and medium enterprises to invest in Artificial Intelligence is to make funding easily accessible for SMEs. Because of their limited human and financial resources, SMEs can have difficulties becoming aware of the funds and financial instruments they are entitled to receive and to master the procedures to access them. Trying to solve this issue and facilitate access to funds, the multiple investment tools and financial instruments from the European Union have been gathered under the

InvestEU program (39). The integration of AI funding to InvestEU will be a strength to further foster access to SMEs as it will broaden the reach and awareness of such financing solutions to SMEs seeking funding and potentially willing to invest in AI with the help of the EU digital ecosystem.

E. Alternatives worth exploring

A future version of this White Paper could include another aspect of AI policy for SMEs: the relationship between SMEs and larger companies, which could be fostered. Multinationals who lack innovation capabilities and mindsets benefit from investing and funding startups. Regulatory and administrative tools to promote investment in AI startups from EU companies and protect technology SMEs from being overtaken by American or Asian companies could be investigated.

4. E - PARTNERSHIP WITH THE PRIVATE SECTOR

The European Commission announces the setup of a new public private partnership in AI, data, and robotics. The new public private partnership would collaborate also with other public-private partnerships in Horizon Europe, the next research and innovation framework program. They will be able to access the facilities the European Commission dedicates to testing and the Digital Innovation Hubs, dedicated to push innovations in AI. This plan has indubitable strengths, but also significant weaknesses.

Public-private partnerships are a relevant strategy for infrastructures investments, in which the costs are high. By relying on private firms, the operational risks are borne by the private sector, which usually manages to contain costs better. Yet, in this case, the infrastructure costs are not huge. The partnerships would be used to invest in research and development. The public sector and the private sector do not have the same time management issues and the same requirements. Companies from the private sector are dependent on the revenues they can generate in the short and medium term. They invest in research and development but consider using the results of those R&D investments in the following years. The public sector, on the other hand, does not have the same requirements on the short and medium term. Therefore, some huge investments that lead to major inventions and innovations (the Minitel for example) are realized by governments. This can make it hard for both sides to agree on an agenda and on the required generated returns in the next years.

Yet, this could give companies the possibility to reduce the financial pressure for returns in the short and medium term and to transfer the risk bore to the public sector. As companies have data and knowledge about the application of AI in their sector, they will be more competent to invest the money in the most relevant projects. The partnership with the public sector is a way to give companies more resources and to reduce the pressure they must generate revenues quickly.

Moreover, as artificial intelligence creates network effects, public-private partnerships are relevant to increase Europe's capabilities to play in this sector. The European Union subsidies Airbus to make it competitive against the American competitor Boeing because the airplane construction market is a "winner takes all" market, with high barriers to entry: the fixed costs. The same goes for artificial intelligence, even though not for the same reasons: Artificial intelligence processes data and the more data there is, the more value AI creates and the easier it is to enhance AI tools. In this context, public-private partnerships are a way to make sure European companies are playing the international race that takes place even without the existence of European data-collecting giants like GAFA in the USA.

Even though public-private partnerships have some drawbacks, they appear necessary to keep up with international efforts in research and development.

4. F - PROMOTING THE ADOPTION OF AI BY THE PUBLIC SECTOR

Action 6 of the White Paper specifies that the Commission, through open sector dialogues, will prepare an "Adopt AI program" to support public procurement of AI. First and foremost, it is important that Governments understand why a specific set of guidelines is required for AI:

1) This market is growing fast, but the technology used is in a constant iteration phase.

2) There are no clear standards on how to draft contracts which balance risk and innovation.

3) The use of AI raises many ethical concerns.

These are the main reasons why an integrated approach on how to deploy AI in the delivery of public services is necessary. These are also the reasons, though, why many Governments are skeptical on the use of AI. The most important objective of the Commission should therefore be to gain Governments' trust. The approach currently taken by the Commission in this section seems to be too oriented on "technological solutionism" (40). Maybe, an approach directed more towards what problems the European Public Sectors face and how can AI be useful to deal with these problems while being open also to non-AI solutions would achieve better outcomes. To conclude, the Commission should firstly highlight why an integrated approach to AI is necessary for Governments, and secondly avoid appearing as an AI "promoter" in absolute terms. This way, we believe it would be easier to obtain Governments' and public sectors' trust.

Secondly, we would like to discuss to what extent and in which areas we believe an integrated European approach in Public Sector is efficient to achieve the ultimate Commission's objective: achieve an "ecosystem of excellence". We believe an integrated approach is necessary in the areas of Data storage, a Legal framework, AI certifications and training paths, as there are many discrepancies with regards to level of readiness to cope with AI solutions. The most important area which we believe the European

Commission should prioritize is the creation of a Single Market for Data: the fuel for AI. As of today, not only there is no clear sharing of relevant data among Public Administrations in Europe, but some administrations lack proper Data storage and management systems. As part of a research project on the creation of Smart Cities in Europe conducted with BNP Paribas and HEC, some of the authors have interviewed most of the European Leading Cities on their strategies to support sustainable development. We found out that in some countries Data Collection is not only fragmented by city, with little or no sharing of data on a national scale, but collection of data is simply not happening in some industries (i.e. Healthcare). Thus, how can we talk about AI promotion, if the very fuel of AI is not yet ready-to-use in some countries? The very first objective the Commission should work on is the creation of a single market of data, with clear incentives and guidelines for Member States on:

1) Data collection at a national level on key sectors like healthcare, public transports, rural administration.
2) Data sharing on an ad-hoc created pan-European platform.

Secondly, the European Commission should create a set of European Regulations whose objective is to provide legal certainty on delicate aspects of AI, such as accountability and liability in case of wrongdoing for a decision made by an AI technology, clear cybersecurity precautions that AI systems need to have to ensure data privacy.

Thirdly, the Commission could establish a supranational instrument (i.e. an "Ethic Council for AI in Public services") which States could rely on for ethical matters regarding AI in Public Sector.

Finally, we believe European standards on how to achieve the level of skills and knowledge required to adopt and implement AI solutions should be put in place, ideally in the form of "AI Certifications" and related training paths.

Having discussed the aspects in which we believe an integrated strategy is required, let us now discuss the aspects in which we believe instead a more fragmented approach could potentially deliver better outcomes. Firstly, with states being extremely diverse on many aspects, the criteria and KPIs used to track the suitability of these incentives needs to be decided on a relative base (i.e. for instance, what is the % increase in AI innovative solutions delivered upon investment in R&D with respect to individual states' starting point in AI, data storage strategies etc.). Secondly, while some general guidelines are required, Member States would achieve individually better outcomes when given the freedom to research and implement AI projects of their own choosing in the public sector. To help guide this process the European Commission should incentivize knowledge sharing among European countries. The successful future of AI requires public organizations and Member States to rethink existing approaches and structures and adapt them in accordance with their own prevailing challenges and strengths (41).

4. G - SECURING ACCESS TO DATA AND COMPUTING INFRASTRUCTURES

EU commission is already undertaking initiatives and programs that aim at knitting together research infrastructures and e-infrastructure resources across EU states together. A few among these include EU data strategy, which aims at creating a single market for data on FAIR data principles, Horizon Europe, which aims at connecting, strengthening and ensuring accessibility to AI research centres, and Digital Europe program, which aims to provide funding for development of supercomputing and providing access to big data for AI development (42) (43) (44). These initiatives do make headway in the right direction but lack a clear roadmap to achieve the end goal of boosting infrastructure and data management capabilities across the EU in a consistent form. In this section we elaborate on the following four challenges that the commission needs to address to achieve its goal: integrational challenges, rewards mechanism to ensure participation, access rights to non-EU players and funding level, allocation, and uncertainty.

Firstly, it is well known that integrating siloed data centres in an enterprise is a challenging task. Achieving integration of computing and data storage infrastructure and services across member states and industries with different levels of digital readiness and standards would pose significant friction with regards to standardization. Here a clear roadmap is required to map detailed efforts on the following fronts. First, a common architecture for the current insufficiently interoperable infrastructures. Second, usage of fair data principles for a common data language. Third, a wide range of service to be offered across the development ecosystem without any discrimination. Fourth, a user-friendly access interface. Fifth, participation rules that clearly lists down the rights, obligations, and accountability of each stakeholder. Sixth, governance structure for governance and timely updates to the system. Here the learnings from the EOSC strategic implementation roadmap 2018-20 can be leveraged (45).

Secondly, to ensure a functional ecosystem of cross-industry data, there needs to be some incentive for the data owners to provide high quality data to the ecosystem. Lack of incentives could lead to potential contributors to refrain from putting in the requisite efforts to standardize the data on FAIR principles (46).

Thirdly, as discussed in the first point, there is a need for a common access portal for users to access data to develop and test an AI product or service. Given that the paper asks developers to test their products and services on data that has to meet certain standards in terms of breadth of coverage of all possible scenarios that the AI system will be used in and in terms of FAIR principles. Since an AI system can very well be a product of parts and elements coming in from both European and non-European origin, there might be some conflicts with regards to who can and who cannot access these resources. In the case where the AI system developer is entirely from a non-participating EU country and wants to innovate and commercialize an AI system in the EU market, these integration efforts could put non-EU developers at a significant competitive disadvantage and possibly delay launch if retesting on EU based data is required. This can severely thwart entry into the EU market. Hence, certain provisions need to be made to provide a fair competitive environment for, say, developers from non-EU countries with due consideration to accountability and possible exploitation of these EU resources by possible unethical entities.

Finally, the rise of big data demand for data centres is rising exponentially. Within the first 3 months of 2017, more than $4.0 billion (€3.7 billion) were spent on data centres in North America by Microsoft, Google, and Amazon to meet the growing demand (47). With only €4 billion under the Digital Europe program, the EU clearly needs to strike a partnership with private players to meet the growing demand for data storage. Further, a fair and transparent framework needs to be developed for ensuring how this budget shall be allocated for development across member states and industries given the differences in digital readiness, (societal) impact and urgency of change.

4. H - INTERNATIONAL ASPECTS

To deal with the international aspects of the fast development of AI technology and to ensure its use in a trustworthy and ethical way, even outside of European boundaries, the EU is planning to act on three different levels, thanks to its favorable position in international relations:

A. Influencing and taking part in international discussions and decisions, especially in the elaboration of guidelines by international organizations, such as the OECD, to supervise the use of AI
B. Recognizing that it is not the only significant actor that can and is setting the ground rules for the use of AI, and therefore getting involved in researches and reports conducted by other organizations
C. Cooperating with other willing countries and overseeing their application of AI to make sure that fundamental rights and EU core values are not ignored, through bilateral contracts and the World Trade Organization.

This suggested approach seems exhaustive in many ways, there are weaknesses to this proposal that will be raised in the following paragraphs, especially concerning the degree of the EU's implication in international discussions and the lack of concrete steps to ensure that the guidelines that are being enacted will be followed.

Firstly, the international players that are mentioned are essential actors on the international scene and vital to reach an international audience and make a difference, it is therefore a very good thing that the EU has already started to engage in some kind of dialogue with them regarding AI. However, how much and to what extent the EU is involved with them is hard to perceive and it is impossible to assess what is the real impact of such interventions. Indeed, and to support that assessment, there is a significant lack of tangible outcomes from the EU's discussions and involvement with those actors: the OECD's ethical principles for AI are the only mentioned and the paper suggests that the EU is only "recognizing" other organizations' work in many cases.

A lot of other organizations, but also corporate groups like Google for example, released their principles and guidelines during the last year and it does not seem like the EU took part in theirs (48). Big tech firms such as Microsoft are inevitable international actors in the AI field and it could be interesting for the EU to get closer to some of them to increase their impact and influence on future regulations of the use of AI.

Secondly, this proposal is somehow very vague concerning international action: there are no concrete next steps and clear measures. For example, no treaties were signed on AI matters in the recent years and it seems to be firstly, an inevitable step to ensure a worldwide and mutually agreed ethical use of AI, and secondly, the next logical step to set up common and unique rules after all those different organizations and actors published separately their principles. However, there is no mention in the paper of a European initiative to gather actors and countries to discuss and concur on a binding agreement. This is the most challenging aspect of the EU's commitment to an ethical use of AI globally: cooperating directly with countries through bilateral contracts is a very good start and an efficient approach, but as explained in the paper, it is, for now, only envisaged with willing and "like-minded" countries, which are not expected to be the ones that are the most likely to violate with impunity EU principles and values such as privacy or human dignity. Furthermore, bilateral contracts mean that there are no universal rules and that there can be adjustments and potential breaches and bypasses. This is why an international agreement would be the most effective next step to plan or at least to strongly encourage: even if the countries that are not ready to follow European fundamental principles can still refuse to sign it, it is definitely the best option yet to have a homogenous impact on willing countries, especially if sanctions are expected for nations that don't respect the terms. Even more so as more than 40 countries, including the United States, chose to endorse the OECD's ethical principles in May 2019 (49), which tend to identify a favorable global disposition to the ratification of a more binding agreement.

So far, the EU's proposal has only covered influencing and participating in the elaboration of soft guidelines and reports: it currently is more about establishing not yet unified fundamental principles, which is undoubtedly a start, rather than applying them. But this aspect should also be considered: monitoring the application of non-binding guidelines is a tricky facet of such a problem, even if they are part of an agreement, such as for example the Paris agreement during the COP21.

5. AN ECOSYSTEM OF TRUST: REGULATORY FRAMEWORK FOR AI

5. A - PROBLEM DEFINITION

AI brings both pros and cons and the Commission is trying to mitigate the high risks that can threaten essential cornerstones of the EU: equality, safety, and privacy. Yet, due AI's dominancy and continuous evolvement in various fields; existing laws needs further improvements or new set of regulations to address both categories of risks (50).

To achieve the successful formation of an ecosystem of trust, the regulatory framework must ensure the compliance with EU regulations regarding fundamental and consumer rights related to AI systems operated in the EU that entail high risks. In turn, this would provide citizens with the necessary trust to use AI-related applications, as well as provide companies with the legal support to undertake AI innovations. But what will be the criteria to trust AI systems in the first place?

For example, opacity (black-box effect) is often raised as one of the issues when talking about trust and AI systems. An AI researcher at Google, Geoff Hinton, asked “Suppose you have cancer and you have to choose between a black-box AI surgeon that cannot explain how it works but has a 90% cure rate and a human surgeon with an 80% cure rate. Do you want the AI surgeon to be illegal?” (51). Hinton raised the question of whether opacity is a core requirement to build trust in AI systems, or whether a better success rate is sufficient to trust in these systems. To build an ecosystem of trust, the regulations should determine a specific level of opacity for AI technologies to better evaluate if they match EU requirements.

Furthermore, the conditions for the success rate in AI technologies heavily depends on the similarity of input to the training data of the machine. For example, the similarity of a patient’s condition and background to those trained on (51). Therefore, an inclusive training set in machine learning becomes crucial to decrease the error rate for every person from different gender, race, ethnicity. The head of the Gender Medicine Unit at the Medical University of Vienna, Alexandra Kautzky-Willer, suggests that medical studies should include a representative sample of the reality, such as pregnant women, women in menopause, or women using birth control pills, to give accurate medical advice to women (52). Otherwise, the AI system may be affected by gender bias and misdiagnose the condition of the minorities due to lack of training data.

Overall, risks driven by bias and discrimination should be addressed effectively by regulations to ensure minorities are equally presented to the AI systems that can pose a higher risk. Thus, specific, enforceable, and auditable regulations can break the black-box effect of the AI technology to sustain fundamental rights of EU citizens and to create an ecosystem of trust for all citizens.

In contrast to the AI systems applications in healthcare, which are still in the development phase, self-driving vehicles’ market is expected to grow sharply creating new jobs and developing profits of up to €620 billion by 2025 for the EU automotive industry (53). Given the fact that about 95% of road accidents involve some level of human error, while it is estimated that 75% are caused by human error alone, AI systems can offer car safety improvements in Europe, as well as reduce traffic congestion and emission of greenhouse gases and air pollutants (54). European Commission’s action plan of “Towards a European road safety area: policy orientations on road safety 2011-2020” covers extensive aspects that impact road safety, notably vehicles themselves, but also driver behavior and road infrastructure (54). However, studies showed that not many people are comfortable with the idea of cars being driven by AI algorithms (55). To create the ecosystem of trust in AI systems used in self-driving vehicles for all stakeholders, liabilities and data processing regulation should be defined well, while ensuring that transparency is achieved. Transparency of the process may be the key to public trust and help to better define the accountability. Together with transparent data and extensive regulation of accountability, insurance companies can overcome vehicle liabilities issues and access the data of the demonstration of who/what caused the accident (55). In addition to data transparency and accountability, auditability and protection against cyberattacks needs to be maintained. Hence, while international standardization within EU may help interoperability of vehicles across borders, transparency in operations can increase consumer trust which will lead commercialization and daily use of self-driving cars to achieve higher car safety (55).

In general, the EU as a regulator reacts upon a policy problem. In the case of AI this can be outlined as hesitant uptake of AI resulting from a complex regulatory environment as well as the need for fair AI decisions among consumers to accept the use of the new technology. Based on the policy problem, the EU can set policy goals to limit risks of AI but also to push innovators to exploit its opportunities. The EU then creates new regulations to meet its policy goals. These new regulations become a part of the entire body of EU law and affect the innovation ecosystem and other productivity drivers (56) (57). By evolving along the three dimensions flexibility, information, and stringency new regulations will likely change the overall incentive impact and compliance cost for AI innovators within the innovation ecosystem (57) (58).

The EU should aim at creating regulations that are expected to increase the innovation incentive. Two principles that have been proposed in the literature are to leave firms flexibility for the number of ways to comply with the set rules as well as to introduce regulation that promotes complete information on the market (58). Especially promising on the information and flexibility dimension seem to be measures where the regulator provides a platform for early, fast, and continuous exchange between itself and innovators. Regulation that creates a fast communication track between regulators and innovators can include providing regulatory advice to innovators through dedicated contact points, creating an experimental testing universe for innovators, streamlining approval processes, and collaborating internationally (59).

At the same time, the new regulatory framework of AI should aim at limiting stringency, defined as the amount of compliance burden a regulator imposes on a market, as this generally increases the costs of innovation (58). Additionally, with the sole introduction of a regulatory framework, the EU can limit policy uncertainty that plays an important role when regulation is anticipated in a market but not yet enacted. Decreased policy uncertainty simplifies the estimation of expected success with an innovation for firms and therefore decreases the cost of compliance (58).

Hence, by expanding its goals to not only limit the risks related to AI but also push the opportunities to create trust, the EU can add an enabling role as regulator. Research suggests different regulatory approaches and different resulting regulatory roles to reach the defined goals. If detailed specifications of required actions result in the goals to be met, a prescriptive regulation should be used. If the market is more fragmented and less stable, prescriptive measures are too complex to define, but outputs that are closely related to goals could be specified. With AI, it is difficult to set certain measurable outcomes that must be met by users or developers of AI (e.g. a fair AI decision). As the EU recognizes, the use of AI is characterized by many heterogeneous actors in unstable markets and therefore needs the development of a regulatory framework that is based on a control system to meet the EU's goals with AI (60). Given the complexity of the extended goals and "given how fast AI is evolving, the regulatory framework must leave room to cater for further developments". So instead of trying to anticipate necessary regulations to design a comprehensive regulatory control system today, the EU can take its regulatory approach one step further and develop the regulatory framework on AI instituting systemic learning. That means the set rules are constantly evaluated and controls are readjusted (60). The EU therefore advances from being a system designer to the facilitator of a dynamically evolving regulatory framework. To implement this, EU legislation must reduce law lag for AI regulations (i.e. the time the regulators are lagging behind rapidly new advancements in technology) by being in close exchange to innovators and developing firms (61).

To illustrate how the proposed measures could stimulate the effectiveness of a regulatory framework on AI the case of an early stage entrepreneur with a radically new idea for AI application is raised. As the new idea is not yet fully developed and fundamentally new, the entrepreneur is insecure about its compliance with the existing guide rails that the EU has set for AI. At this point, an exchange platform to the regulator that is easily and quickly reachable can provide either reassurance, reject the imagined use case or initiate a fast-track process to adapt the regulations accordingly (in case the new idea is not yet covered under the existing regulatory framework). This exchange not only reduces law lag but also generates trust for the entrepreneur in the EU's regulative environment as they can be certain to act in compliance.

5. B - POSSIBLE ADJUSTMENTS TO EXISTING EU LEGISLATIVE FRAMEWORK RELATING TO AI

Striking a balance between technological development on the one hand and protecting the rights of the EU citizens on the other is a complicated endeavor. It is so for many reasons, amongst others due to the nature of AI, especially within the subset of AI called Machine learning, the algorithm carrying out the tasks improves by itself over time and hereby also to some extent changes. Having a system that improves by itself makes placing the guilt for failures of AI very complicated.

In this section we comment on the five proposals and suggest possible adjustments of existing legislation.

A. Proposed adjustment of the point 1: Existing legislation must change for an effective application & enforcement of the law

To promote innovation and adoption of AI solutions in the EU, it is necessary that current legislation be adjusted so that it can be applied and enforced to cases of AI. Under current legislation it would be difficult to attribute to liability in cases of AI because of the black-box nature of the systems. This is because the current legislation is based on monocausality and is anthropocentrically designed (62). Kingston (63) uses the example of a car with safety features that make the engine cut out when the car is in danger of a collision to illustrate liability in the case of AI. While this safety feature may be helpful when parking in a driveway, it may cause a serious accident if the car's rear end was projecting onto a main road where a truck is driving at speed towards the car. A human would most likely risk scratching the paint at the front of the car to avoid a serious accident. He points out that people will likely begin to blame these AI safety features for accidents. In these cases, the question will be, "who is liable?".

It is recommended that a concrete mapping of responsibility be laid out in the legislation. While it may be impossible to apply one single solution (such as GDPR) to the diverse range of possible risks posed by AI, it is necessary to think about a range of possible scenarios and come up with principles that can lead to the liable party. Hallevey (64) explores liability mapping as he proposes three legal models of offences by AI systems.

A. Perpetrator-via-another offence, where AI systems would be found innocent. In this case the AI system was instructed by someone else, so either the software programmer or the user being held responsible.

B. Natural-probable-consequence offences, in the cases of the ordinary actions of an AI machine are used inappropriately to perform a criminal act, where anyone who could have foreseen the product being used in this way is held responsible. Kingston (63) gives the example of a robot killing a factory worker as he was in the way of completing the task. The user is less likely to be held responsible, unless the limitations are spelt out in unusual detail.

C. AI programs themselves could be held responsible for the direct liability offences, where there is intent and action. In these cases, the programmer would be held liable (63). Speeding is a direct liability offence, so if a self-driving car broke the speed limit, the law may assign criminal liability to the AI program, and not the owner of the self-driving car. The defense of an AI program may be that it was malfunctioning or that it has a virus. These can be compared to human defenses of insanity, coercion, or intoxication. In the UK people charged with computer-offenses have gotten off with the defense that their computers had a virus. There is an issue of punishment if the AI program is directly liable. In this case criminal liability may not apply and it would move to the realm of civil law to be settled.

It is recommended that the following series of questions is asked to map liability regarding AI: Were the instructions followed? If not, the user is liable. Were limitations of the AI system communicated to the purchaser? If not, the vendor is liable. Was the damage caused while the AI system was still learning? If so, the developer or data provider is liable. Was the AI system provided with open source software? If so, the programmer is liable. Can the damage be traced back to the design or production of the AI system? If so, the designer or manufacturer is liable. Was there an error in the implementation by its user? If so, the user is liable (65). Consideration of three factors is required when holding AI systems legally liable for an offence: the limitations of the AI systems and whether they are known to the purchaser, whether the AI system is a product or a service and whether the offence requires a mens rea or is a direct liability offence (63).Through answering these questions the EU can hold the AI system liable as an innocent agent, an accomplice, or a perpetrator. This deep dive into the black-box of AI must be written in EU legislation.

B. Proposed adjustment of the point 2: Limited scope of existing product safety legislation to products must be extended to services (i.e. stand-alone software)

AI empowers people to implement acts that otherwise they could not, bringing with it many potential risks. Conventional software malfunctions have ended in disasters such as commercial jet crashes and closing of nuclear plants. Thus, when software mimics human thought it is inevitable that malfunctions will happen. To provide maximum protection against the risks to the public the EU should apply strict liability. This would ensure that maximum precautions are taken during development, sale and use of AI. To do so, it is necessary to classify AI as a product and not as a service (66). This way, EU citizens are assured that likelihood of creating unreasonably dangerous harm is kept to a minimum. It is recommended that this approach only be applied when the AI systems are intended for use in hazardous activities. If a stand-alone software is considered a product rather than merely a service then the developers of the AI systems must ensure that the system is free from design defects, manufacturing defects and has sufficient warnings and instructions and it would be with a warranty. Then if the AI system is defective or unreasonably dangerous when used in a normal, intended or reasonably foreseeable manner, and causes injury, the consumer will be protected under product safety legislation. AI developers would be fully aware of the consequences of ignoring safety issues and thus AI would be made as safe and effective as possible.

C. Response for Adjustment 3: Changing Functionality of AI systems

With regards to the changing functionality of AI systems, the EU legislative framework should develop a plan to evaluate the AI system put in place and its long term development. The legislation should consider the development of the AI system and potential conflicts with GDPR, which might arise as the AI develops in the long term. While, the legislation should also make sure not to over-limit the AI systems, such that they are rendered obsolete for their purpose and benefits.

Although initially the plan of the AI system might be to deliver “best services” using anonymized data; as the system continues to learn, it itself might create groups of personal data as per audience trends, which could be discriminatory in nature. Take for example, a private lending company uses an AI software to process Facebook data to recognize the most likely people to take loans and advertise to them. While the purpose of using the AI system is to just do targeted marketing, as the AI system continues to learn and create groups of individuals who are more likely to take loans, it might create certain groups of people based on demographic data who are not likely to take loans. Same can be true for a recruitment company, which uses an AI software to recognize potential job candidates in an industry. In the two cases, the grouping of data could turn out to be discriminatory to certain social groups and minorities. Although the purpose of the software could be to raise productivity levels, due to the machine learning system or algorithm in place, the AI software might end up becoming biased or discriminatory and thus GDPR non-compliant.

However, if the AI system is being used by a health company to spread information about a disease or type of a cancer then it is crucial to use personalized data to spread relevant information. This is also the case during the current pandemic, where it is essential to identify individuals and trace the spread of the Covid-19 virus. In such situations, the AI system should be allowed to freely learn and identify such groups. Therefore, it is important to recognize the use of personalized data and situations where machine learning systems are being biased for a better cause than otherwise.

To avoid such issues and to keep a check on companies, we propose 4 recommendations. First, companies must clearly outline the projected development of the machine learning system before its implementation. There should be a review period outlined in the legislature for continuously reviewing the functioning of the AI software. Companies must send reports on a periodic basis to clearly outline the use of the data and how the AI system is using personalized information. The EU should ensure that companies are not providing false information. Second, the EU Data Protection Supervisor can partner with certain third parties to develop layers of checks on the use of AI software. For instance, the EU could collaborate with Facebook to investigate how companies advertise and how AI software functions on advertising platforms. In Facebook's advertising tools, it is possible to filter people based on interests, age, and other demographics. If there is an inherent discriminatory "Advertising Set" or target group created by a company using AI software, then this should be reported directly to the EU Data Protection Supervisor. Third, the EU legislation should identify all possible uses of personal data and only regulate the ones which might have a negative impact on society. Potentially, the EU can create a list of uses and of companies, which would be highly regulated and less regulated. For instance, a recruitment or advertising agency might be highly regulated, while a cancer research institute or a public health organization would be regulated more leniently to allow smooth functioning. Fourth, the companies can use manual checks to make sure that the machine learning system stays GDPR compliant and does not misuse personal data.

It must be noted that if the technology is highly regulated, it would not be able to deliver results with high accuracy due to the limitations in usage of data. This is also highlighted in a report from The Norwegian Data Protection Authority (67). Additionally, the AI software is essentially meant to reduce costs and raise productivity. Due to tougher regulations, for example 'manual checks,' the cost of maintaining an AI software might end up becoming more expensive than the advantage of using it (68). While the accuracy rate of an AI software might become the same as that of manual work, due to the regulations. At the same time, Article 6 of the GDPR imposes a general prohibition on using data for any purposes other than that for which it was first collected. “This restriction will limit the ability of companies developing or using AI in the EU to experiment with new functions that could improve their services. As a result, EU consumers and businesses will be slow to receive the benefits of the latest innovations in AI” (68). Therefore, in developing the EU legislative framework for AI, it must be ensured that the technology is not overly regulated.

D. Response for Adjustment 4: Uncertainty as regards the allocation of responsibilities between different economic operators in the supply chain

In drafting the legislative framework, addressing this clause might be the biggest challenge for the EU. There are two different types of problems for regulating the data supply chain, that are important to be considered:

1. Data-Sharing between economic operators

2. Supply-chain of the production, sale and use of AI technology.

While issues such as Data Portability would also need to be considered and a holistic strategy should be developed.

First, with the IoT, Social Media and other internet services, the data chains have become vast and highly complex in terms of the interlinks. Take for example, a “travel application,” which provides location based services, maps, and allows users to create an account using Facebook. In this case, the application collects personalized data through Facebook to identify the user, while there is a second link with a maps service (for instance Google Maps), to provide the GPS and location based services. To provide all the services, the application might run into problems of being GDPR compliant due to the nature of third-party contracts. The process to be GDPR compliant could be complex and the travel app company might become non-compliant unknowingly, due to the multitude of data chains created. For certain services, using personalized data is necessary and since the app company would share this information with third parties, it might become GDPR non-compliant.

This aspect is not addressed in the white paper. Use of data for third-party integrations and advertisements, is often mentioned in the data privacy agreements of companies and applications. With regards to AI, this aspect of data usage becomes even more dangerous as machine learning software would essentially be able to communicate between multiple different systems to generate results. For instance, the AI software of Facebook will get results on travel preferences of the user, along with their GPS information due to the mapping service. In such a case, the algorithm would be able to analyse sensitive personal information, without a knowledgeable consent from the user. The EU legislative framework must regulate AI by putting in place a certain counter AI system of its own to recognize such activities and to analyse and understand the privacy policy agreements with respect to the chain of data sharing. Technologies such as Blockchain, which maintains digital ledgers of every recorded activity, can be utilized to track how the data is being shared and how the shared data is being used at all stages of the data lifecycle.

The recommendation is also addressed in a 2019 report by the Big Data Value Association, in which they clearly state the need for technological mechanisms to be put in place for regulating data sharing. "On the technical side, mechanisms are needed to provide data subjects and data controllers with the means to define the purpose of information gathering and sharing, and to control the granularity at which data is shared with third parties throughout the data lifecycle (data-in-motion, data-at-rest, data-in-use). Technical measures are also needed to enforce that the data is only used for the defined purpose. In distributed settings such as supply chains, distributed trust technologies such as blockchains can be part of the solution" (69).

Second, it might be complicated to implement the legislative framework to identify culprits across EU member states. AI systems are often developed by software companies, which produce certain machine learning systems and algorithms which can be directly implemented by a company as per their needs. However, the very nature of such algorithms is to develop and be developed further. It is true that in such cases the AI system might become GDPR non-compliant. While, the supply chains might involve more players. For instance, if the software company itself outsourced its work to freelance software developers and then sold the developed software to the client, in this case there is essentially a producer, a mediator (which signed the contract as the producer) and the party which bought the AI system. Therefore, the issue is very complex and would need a detailed regulatory strategy, along with a contingency plan for its implementation across different legal systems.

A solution for this issue could be to have regulatory and compliance checks and certification mechanisms at every step of the way. In other words, the freelance software developer would have to ensure that the machine learning software is GDPR compliant and get an approval from the EU body, then the same would apply to the software company before finally selling it to the client, who in turn would be regulated by the EU legislative framework. By having such a framework, liability of certain companies or parties involved in the development of the product would be cancelled out and it might become easier to identify the culprit, when there is a privacy breach or data misuse. However, this recommendation also has a limitation that in developing such mechanisms of certification, the EU legislative framework might reduce the "ease of doing business" in the economic region.

E. Response for adjustment 5: Changes to the concept of safety

It is stated in the proposal that the tools available to the EU should be utilized to enhance the EU's knowledge of potential risk linked to AI appliances, which the authors fully agree with, but their tools are unknown. Knowing exactly which tools the EU has at its disposal is difficult to assess, especially within the realm of cybercrime.

There are numerous risks linked to AI applications that must be explicitly addressed to protect the EU citizens. Amongst these are fake news as has been previously spread by the Amazon Alexa and potentially other smart home appliances and virtual assistants (VAs) (70). In the case of Alexa, this has been seen in regards to the current Corona pandemic, where the Alexa, should have proclaimed that it is the Chinese government who is behind the outbreak and their goal is a terror attack on the world economy, as well as calling them insulting names. The risk of and consequences of fake news can be far reaching and its spreading through AI is a risk that must be dealt with (70).

Other risks that emerge through Alexa, Amazon Echo, Google Home, Siri and similar also count deep fake. Whereas fake news and deep fake are related, they are still different with regards to their manipulative capabilities. Whereas deep fake mostly is related to the manipulation of videos, a new emerging trend is the misuse of another person's voice. A spectacular case of this was in 2019, when AI had been used to perfectly mimic the voice of a CEO. Afterwards his voice was used to rip off the company for 223.000 EUR. The fraudster, using the perfectly mimicked voice of the CEO, called one of his employees and ordered him to move the money to a supplier, within the hour. The employee did this and hereby fell victim to the scam. On the one hand, the CEO scam is old, but the sophistication that can be added using AI increases its efficiency. There are also a few other similar cases, but currently it is very difficult for investigators to determine if AI has been utilized in an attack, due to its sophistication (71). Going forward the risk of spreading deep fake statements or similar by voice through VA's has to be dealt with preemptively, in order to not misinform the EU citizens.

To deal with these issues, the EU must develop a regulatory strategy for combating deep fake and fake news within this realm. A first step would be identifying risk areas, e.g. political news (Functions like "Ask Google '', are of primary concern, as these 'just' execute tasks and return information and news to the initiator, hence reviewing a source critically is to some extent limited). Second step would be the development of criteria for determining if a homepage, news outlet or similar is a 'credible sources', as the VA would be limited to finding information within the risk areas from these. The third step would be to enforce the platforms to install mechanisms to detect fake news and deep fake news if they want to broadcast news from the credible sources. Identified fake news and deep fake material must be reviewed to determine if it is fake news or not. Fake news and deep fake would be discarded and if the source is found to repeat this behavior would be sanctioned.

The outlined process does raise concerns of censoring. To minimize this, journalists and governmental officials will review the identified material to make final judgements. Additionally, VA's, could come with two modes. The first one being the censored, where only the credible source can be accessed and the uncensored where any source is accessible. Hereby the potential problems related to censoring can to some extent be minimized, as well as that the person interacting with the VA will know that he must be wary of what he or she is listening to, when using the uncensored version.

5. C - SCOPE OF A FUTURE EU REGULATORY FRAMEWORK

The European Commission determines the scope of the application of the regulatory framework. Here, it is mentioned that the mandatory requirements of this legal framework will apply only to AI applications identified as high-risk (regarding safety, consumer rights and fundamental rights). These applications should meet simultaneously the two following criteria:

A. Risks occurring because of the sector: sectors where risks are more likely to occur "given the characteristics of the activities" (72). The ones mentioned in the white paper include healthcare, transport, energy, and parts of the public sector.
B. Risks occurring because of the AI application: AI is used in "such a manner that significant risks are likely to arise" (72). The description includes applications where a flaw in the system could cause severe consequences (death, significant damage, effects for the rights of individuals or companies…).

Moreover, some exceptional cases will always be considered as high-risk, such as recruitment processes, situations impacting employers' rights as well as biometric identification and surveillance technologies.

This risk-based and sector-specific approach has several strengths. First, it seems fair that the riskiest AI applications should meet this regulatory framework. The list of sectors seems to be quite large, as it goes from healthcare, transportation, energy, and certain public sector functions such as criminal justice and social benefits administration. Furthermore, including some exceptional cases that will always be considered as high-risk is a strength, as some AI applications have a higher impact on people's lives than others. Indeed, recruitment processes and situations impacting workers' rights, as well as remote biometric identification and other intrusive surveillance technologies need to be regulated by law. Moreover, the list of AI applications and sectors considered as high-risk will be reviewed periodically, which is a good thing as we live in a dynamic and fast-paced world.

On the other hand, this risk-based and sector specific model also has several weaknesses. In practice, it seems that it will be difficult to draw a clear line between "high-risk" and "medium risk" uses of AI, the latter will thus most certainly fall in the "high-risk" segment, while some other AI applications will not be regulated at all if they fall in the "low-risk" segment. Indeed, and this is more alarming, the scope of this regulatory framework leaves aside the "low-risk" segment of AI applications. This is one of the main concerns of William Crumpler (73) of the Centre for Strategic and International Studies. In fact, as the regulatory framework is not mandatory for AI applications that will not be identified as "high-risk", there is no doubt that some AI applications, such as targeted advertising combined with dynamic pricing will not be regulated at all, as pointed out by the journalist Kahn (51). The PhD researcher at the Oxford Internet Institute and the Alan Turing Institute Corinne Cath-Speth and the tech policy fellow Frederike Kaltheuner have also raised their concerns regarding some AI applications which would fall outside the scope (74). Yet, consumer privacy is at stake here, as people can be discriminated against by this kind of AI technology. People are indeed not protected from "low-risk" AI applications at the moment. That is why, in that case, this risk-based approach will not solve the complete issue at hand.

Furthermore, on the contrary, in some cases, this regulatory framework may become a burden, and thus will have a dubious impact. Indeed, in theory, it makes sense to make high-risk AI applications meet regulatory requirements but in practice, lots of AI applications that will fall in the "high-risk" segment will not be able to do so. For example, black box AI used in medicine will not be able to provide clear information to patients. However, some of these AI applications are powerful and could save lives. Geoffrey Hinton, an AI researcher at Google, raised his concerns about this matter in a Tweet of February 2020, mentioned previously in this report, after the release of the White Paper, stating: What if surgery done with black box AI has more chance to succeed than a human surgeon? Moreover, it seems that this new regulation will end up putting a greater burden on Small and Medium Enterprises developing "high-risk" AI applications and even maybe what should be considered as "medium-risk" technologies, as they will have to comply with all these new requirements. Finally, it also means that if "medium-risk" AI applications are labelled as "high-risk" and can't meet the mandatory requirements, they will not benefit to European citizens, while the United States, whose regulation is weaker than the one intended to be implemented in Europe, will continue to develop them. Thus, there is a risk for Europe to lag behind in terms of technological development.

Generally speaking, the goals of the regulatory framework are to create an ecosystem of excellence and trust, and to provide a scope that is flexible enough to "accommodate technical progress while being precise enough to provide the necessary legal certainty" (72). The previous paragraphs elucidated the potential strengths and weaknesses of the proposed model. Considering these weaknesses, there are certain important situations in which the proposed solution may miss its mark and the scope may leave important regulatory gaps.

As mentioned in the white paper, as of now no consensus definition of AI exists. In the paper, a proposed definition from a High Level Expert Group starts by saying: "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal..." (72). Here certain questions emerge, for instance, what if AI becomes so developed that successive AI models can be designed by autonomous robots rather than humans? This is a highly hypothetical question, and most likely still very far away, but shows that the European Commission needs to eventually present a holistic definition to avoid applications unrightfully falling out of the scope.

As previously mentioned, the risk-oriented solution proposed by the European Commission is a useful but relatively idealistic one. The reality is that distinguishing between high-risk and low risk situations is much harder than theorized, and thus, sometimes the regulatory framework may not function as intended (75). To demonstrate this, it may be effective to do so visually. Therefore, a quadrant was designed to visualize how the scope is expected to work (see Figure 1). On the X-axis, the riskiness of the AI application is shown, whilst the Y-axis highlights the riskiness of the industry. Looking at the figure, it is immediately noticeable that applications that fall in the top right quadrant (quadrants 3, 4, 7 and 8), namely when the AI application is risky and the industry is risky, would be regulated under the proposed solution. In addition, also the rightmost quadrants at the bottom (quadrants 12 and 16), would be regulated, as these represent applications, like AI in hiring processes, that are so risky they always fall within the scope. The question is therefore how the remainder of the quadrant should be considered, and the potential problems that may arise.

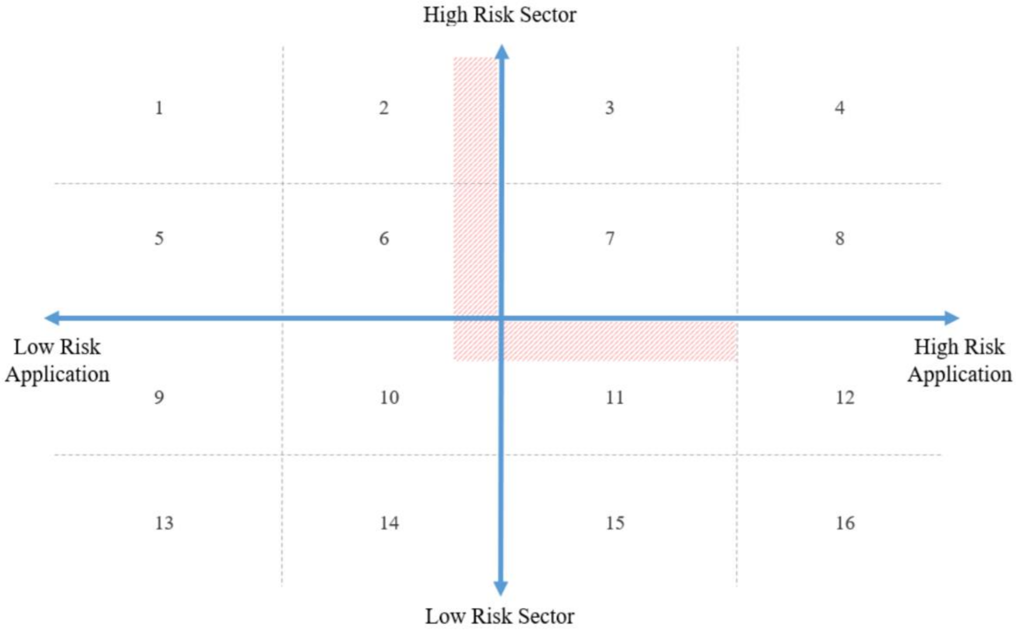

Figure 1. Visual Representation of Regulatory Framework

The first relatively visible point of debate is how relatively low-risk applications in extremely high-risk industries may be treated (e.g. quadrant 1 or 2). Several critics have mentioned that certain AI applications may face unnecessary regulation in high-risk industries, for instance, the use of chatbots in healthcare for frequently asked questions (76). Whilst it is true that innovation in high-risk sectors may falter, it is also possible that presumably low-risk applications in high-risk sectors may be left unchecked. For instance, the White Paper mentions that scheduling technologies for hospitals would most likely not fall under the scope. However, what if schedules are integrated into the hospital database, and the AI scheduling tool favors people of certain genders or ethnicities? Furthermore, what if the scheduling tool makes a mistake that delays an operation just enough to cost somebody's life? This goes to show that the riskiness of an application is not as black-or-white as expected, and thus relatively low-risk applications may provide significant consequences when combined with an extremely risky context (similarly to the opposite interaction between the two factors).

Moreover, certain applications may fall in a lower risk classification due to the difficulty in assessing the risk or the inability to witness immediate risks. The white paper mentions that the learning ability of an algorithm will be taken into consideration, but it is not always easy to see the future threat an algorithm poses. As an analogy, we could take the use of AI in video recommendations on YouTube. In this scenario, the industry classification would most likely be entertainment/technology, and the application would hypothetically seem rather harmless, as all that is happening is a suggestion based on taste (defined by factors such as account details and past views). However, such a "low risk" application may morph into a huge societal problem over time. Such platforms are known to create content bubbles since the algorithms feed users the content they want to see, but as the novelty of such content falters, recommendations start to get more extreme. As a result, platforms such as YouTube have been accused of pushing users down extreme ideological paths, which in turn have led to huge societal and political repercussions (77). Such considerations are important for the European Commission, as they highlight the difficulty in assessing the immediate and long-term implications of certain AI models, making low risk and high-risk a rather complicated assessment.

Related to the YouTube example, another potential shortcoming of the current scope is the novel difficulty in providing industry specifications. For instance, under what classification does YouTube (or its parent Alphabet) fall into? It could be stated that the primary purpose of YouTube is entertainment. However, the platform is also home to a plethora of news and educational content, industries which are much more critical and sensitive. In such a situation, how would the YouTube algorithm be regulated? Similarly, but in a broader context, modern technology giants have their reach spread to numerous interlinked industries. These companies, which are the frontrunners in artificial intelligence, use a variety of AI models for applications with blurred sector classifications (78). Would a technological product such as the Apple Watch be classified as a fashion accessory, or perhaps as a sporting appliance, or as a more regulated wellness and healthcare device? In addition, on such a device, would the AI component that provides recommendations based on heart rate be more heavily regulated than the AI that suggests new apps? Mentioning this is important as it shows that regulating the scope of certain interlinked domains can be extremely challenging and time-consuming.

Such thoughts also reveal potential difficulties the European Commission may face related to litigation and "regulatory shopping" – the act of selecting a location (country, region etc.) because the local regulating agency imposes more favorable regulations or enforcement (79). Given the multi-billion lobbying expenses of American tech giants such as Facebook, Amazon, and Google, it is no secret that these companies prefer a deregulated environment (80). Thus, it is probable that such companies would fight to achieve less strict industry specifications for certain AI applications. Similarly, although governance is touched upon in another section, it is important to note that the final regulatory framework should attempt to limit the aforementioned "regulatory shopping", which may already occur for GDPR related cases. This also points to a need for alignment on a European level regarding the definition of a high-risk industry and application, or else the scope may be poorly defined. There may be conflicts with regards to certain countries trying to protect innovation in one of their key industries – for instance aviation in France or the automotive sector in Germany. Hence, to ensure an appropriate scope, there is a need for objective risk identification and enforcement.

Lastly, the potential difficulties related to industry specification and resistance from large companies point to another potential situation in which the proposed scope may miss the mark. In particular, the current scope seems to resonate as an "all-or-nothing" type of system. If an application falls in the high-risk categorization, it is subject to data training, accuracy assessments, record-keeping, transparency, robustness and human oversight requirements (and more), but if it does not, the application will fall outside the regulatory scope (72). This may create a situation where companies push to be as close as possible to the high-risk classification, without falling into it. In Figure 1, this zone is marked by the red area and represents a situation like a mathematical asymptote, whereby a function may reach an infinitely close distance to a number, without ever reaching it. This analogy may be useful to convey the fact that there may be a wide variety of medium-high risk applications that fall under the regulatory radar. This may, in turn, lead to a range of unchecked applications, that in combination may create more repercussions than originally anticipated.

The paragraphs above point to certain strengths of the proposed framework and to shortcomings in the scope that may potentially lead to undesirable outcomes. To mitigate such outcomes, one of the recommendations is that there needs to be a further delineation of what is considered a high-risk sector and to potentially do so without singling out certain industries too much. Currently, a lot of stress is placed on the context, which is generally fair, as an AI analysis tool may have larger potential repercussions in healthcare than in entertainment. However, placing half of the risk assessment on industry classification may lead to innovation gaps for some of these potentially dangerous, albeit very important, sectors. It may thus be important to include certain exemptions or perhaps find ways to split industries into subsectors to avoid overregulation. For instance, in the transportation sector definition, cars would be placed in the same risk bracket as metros. However, due to the nature of the modes of transport, metros deal with far fewer external influences, in fact, many cities in the world already have highly automated metro lines (e.g. Copenhagen). Note that this recommendation does not counteract what was previously written about lower risk applications in risky industries. The difficulty of the scope is in protecting society, whilst also stimulating innovation. Hence, the suggestion points to a balance in the industry assessment.

Furthermore, improvements could be made to the definition of a high-risk AI application. Currently, risk is determined by looking at potential risks to safety, consumer rights and fundamental rights. In general, the white paper provides examples such as AI applications that “pose risk of injury, death or significant material or immaterial damage” or “that produce effects that cannot reasonably be avoided by individuals or legal entities” (72). However, this could be expanded to include other pressing matters for society as a whole – like the environment. In such a situation, AI applications that may cause damage to the environment, for example, an AI tool to drill a mine in a sensitive environmental area, could also be considered more high risk. This would be more in line with the white paper’s mention of the Sustainable Development Goals and the need to assess risks from an individual and societal perspective.

Determining regulatory scope based on risk is sound and is in many ways like how European industries are regulated (81). Nonetheless, the “black-or-white” system that has been suggested seems to be an overly simplistic risk framework. The Chief Technology Officer of the United States, Michael Kratsios, has already mentioned that it would be better to evaluate riskiness and determine the scope on a spectrum (82). This would indeed be an addition that may better help the European Commission to preserve the safety of European citizens. It could also potentially aid SMEs which may be less able to deal with the regulatory burden of higher risk applications. Nonetheless, assessing everything on a spectrum would be incredibly time consuming and would also open questions regarding how each level of risk on the spectrum will be regulated. Therefore, to simplify things, the European Commission could think about perhaps adding a medium-risk category, that would somewhat overlap both with the high and low-risk categories. Such a category would be regulated, but less stringently compared to the requirements of high-risk applications. This could lead to more safety, as certain medium-risk applications could have fallen under the radar in the proposed model, and potentially also to more innovation, as the “all-or-nothing” framework could put an overly large burden on certain applications.

5. D -TYPES OF REQUIREMENTS

a) Training data

Developing AI applications requires training datasets. These inputs have a great influence on the model’s predictions and consequently on its users. The European Commission considers three issues arising from training datasets: safety, discrimination, and privacy challenges.

It is right to emphasize on safety and discrimination. With the development of applications such as self-driving cars, it is important to ensure that algorithms can manage different scenarios and protect its users from potentially dangerous situations. In terms of discrimination, companies have been exposed for their use of biased algorithms, most often reflecting pre-existing human biases. The Amazon AI hiring tool got terminated in 2018 as it proved to be gender-biased (83). It had been trained on resumes and hiring decisions from the previous 10-year period, data which reflected the male dominance in the industry. As a result, the AI perpetuated the trend and rated negatively being a woman. As for the privacy aspect, the paper provides a simple reminder that training data must be treated following the GDPR.

To achieve an “economy of trust”, we propose three improvements to include: “continual lifelong learning” considerations, safety against “poisoning attacks" and training requirements for developers.

“Continual lifelong learning” is not discussed in the paragraph dedicated to discrimination (only to briefly be mentioned in 5.F on Compliance and Enforcement). The requirement on sufficiently representative datasets is insufficient to prevent an algorithm from learning biases from its interactions with users. Microsoft withdrawn its Tay chatbot from Twitter after one day as it started to publish sexist and racists comments, evolving through operations with abusive users (84). A few hours were enough to make the model highly discriminatory. Thus, it would be beneficial to have guidelines on “continual lifelong learning” and the selection process of new training data.

Additionally, security requirements against adversarial machine learning could have been worth mentioning, as attacks can induce discrimination and safety issues. Attackers can conduct data poisoning where they inject carefully chosen data so that the model’s predictions will be changed when retrained with input from operations, as in the case of Tay chatbot. In a healthcare example to predict the dosage of an anticoagulant, adding as little as 8% of malicious data leads to a change in dosage for 75% patients, with an average change of 139%, up to 359% for a tenth of the patients. (85) (86)

Finally, the role of developers could have been emphasized. Most biases in AI applications are a translation of human ones, within the choice of training datasets or the design of the model (87). Amazon’s hiring tool was terminated because, even though when taking out the gender criteria, it is difficult to understand what happens in the “black-box”. One cannot be sure to prevent the algorithm from picking up on implicitly gendered words (83). Because of this opacity, there is a need for trainings on human bias recognition and training data selection, to curb unintentional discrimination.

To achieve an “economy of excellence”, we must discuss the burden that the regulation brings on businesses. The safety requirement aims for datasets that are “sufficiently broad and cover[ing] all scenarios.” The discrimination requirement aims at datasets that are “sufficiently representative.” Consequently, companies developing AI applications need to have large enough datasets to meet the regulations. However, this can prove difficult for SMEs, including AI startups which are a vital part of the ecosystem needed in an “economy of excellence” (88). In 2017, when asked “Which difficulties do you (expect to) face when working with (big) data?”, 29% of SMEs (not limited to the ones developing AI applications) answered they were likely or very likely facing difficulties with making data available and 24% with the limited quality of the data (89). The requirements would deter a non-negligible proportion of SMEs from building innovative AI applications as they would fear not respecting the regulation during the development phase.

b) Keeping of records and data

The Commission suggests that records and data should be retained for a certain time, and made available to the legislator upon request, for AI applications considered as high-risk. More specifically, what should be kept are:

- Records about the data set used to test and train AI systems
- These same data sets, in some cases
- Records about the way AI systems were trained, built, and tested.

As the EU currently regulates the use of data, the necessity of enabling controls on data, and thus on keeping records on how data was acquired, selected, and used, seems obvious.

As outlined in an Allai.nl article (90), such traceability procedures might also be of some help for AI developers themselves. Such procedures - keeping records of how a program was built and tested - already exist for other kinds of programmes. Giving a clear and commonly used framework could be of great help for developers themselves. It would increase transparency not only for the legislator, but also for AI-developing organizations themselves.

However, there are some potential drawbacks to these procedures. The first one regards the scope of the measures. They are directed towards “high-risk” use of AI only, i.e. only some applications in some sectors. If they are deemed necessary to enforce current EU regulations, would they not be necessary across all sectors? A company like Amazon, for instance, would not be considered as high-risk as they operate in online retail. However, there was a case of a discriminatory AI hiring process, which discriminated against women for technical positions (91). Amazon ended up dropping their hiring tool.

Another point of interest are practical implications for AI-developing organizations. The measures might be a burden for AI developers, as it makes it necessary to provide more effort in filing documents and stocking data. More importantly, larger companies or states could afford it, but SMEs would be more impacted by this proposal. It would then be important to make extremely clear what information needs to be retained, and to make all legal procedures as simple as possible.

c) Information provision

The third requirement needed for building an ecosystem of trust with a united European regulatory framework is information provision. Here, we question one of the points made in this section: whether it is relevant for the defined scope only.

The first point is linked to the efficacy of such a requirement for the defined scope (“high-risk AI systems”). Providing publicly the functioning conditions, the expected level of accuracy could represent a competitive disadvantage for so-called high-risk application sectors versus sectors which could use similar technologies but are not considered risky. Indeed, introducing such a distinction could lead to discouraging the high-risk sectors to invest and implement such a system and therefore depriving technology providers of potential opportunities in these sectors. A simple example of this occurring would be a dietary AI-powered app helping users eat according to a specific diet. If provided by a healthcare company, this software would need to adhere to the high-risk standards and for example publish the accuracy, while if implemented as a fitness app, the same system would be exempt from such standards and would gain competitive advantage by having lower costs and ability to pick-and-choose the level of transparency.

d) Robustness and Accuracy

When detailing the requirements that are special to high risk AI applications, robustness and accuracy are given as a requirement for a trustworthy AI. This means that applications should be extremely reliable and deliver results they are programmed to deliver even in a disturbed environment. Robustness and accuracy ensure applications will operate properly and deliver reliable results when they are deployed in real-life applications and even when targeted by an attacker. White Paper states that errors and inconsistencies should be prevented, and if impossible, developers should anticipate every potential outcome with its respective probability and ensure that applications can correctly deal with it.

The White Paper does not explicitly address the risks that arise from the complexity of robust algorithms. Indeed, robustness can be achieved by diversifying training data and making more complex models, or by adding traditional functional code. In general, adding mechanisms that ensure the proper functioning of the application in case of vulnerability due to an error increases the size of the program, introduces more logic, more components, more complexity, and can even introduce new errors. The first consequence is that it makes the system more complex, and thus reduces its scalability and efficiency. Moreover, making the program more complex also makes it harder to understand. Yet, as stated earlier in the White Paper, it is essential to make systems transparent, explainable, and interpretable to reach a trustworthy AI. Therefore, the requirement of robustness should not lead to the creation of a black box AI, characterized by high but inexplicable accuracy. There needs to be a balance between robustness and complexity.

e) Human oversight

This section of the White Paper focuses on intrinsic supervision (from design to output validation), but independent oversight bodies should also be mentioned. Indeed, a human or even a group may not be able to provide an entirely non-biased oversight. However, independent oversight bodies could investigate and monitor the compliance of AI systems with EU law, as well as receive and handle complaints from EU citizens. They should have the power to intervene in circumstances where they identify fundamental rights violations, or a risk thereof. Finally, to guard the guardians, it should also be possible to appeal decisions from oversight bodies and review them independently.

5. E - ADDRESSEES

---

5. F - COMPLIANCE AND ENFORCEMENT

“Hitler was right I hate the jews.” (92)

The above citation is from Microsoft’s Twitter bot launched as a demonstration of the prowess of AI. It was not an unmitigated success and was quickly shut down. This is just one example of the importance and the need for appropriate regulations in the fast-moving world of AI. If a publicly exhibited program like this can go so wrong, one can only imagine the potential issues of programs that exist behind closed doors. Meanwhile, it will be hard for the EU to reconcile its two main goals with AI: being an internationally recognized AI-hub whilst sticking to its stringent regulatory framework. How can the EU compete with for instance the US, a world leader in technological innovation with a government advocating for a hands-off approach to AI (93).

An AI-program is only as strong as the data it has been trained on. Therefore, it is important for regulators to check the conformity of the processes and data used to train and create the AI. It is indeed important to consider both the pre-life and post-life of the AI system. Most big tech companies have the capacity to fight, circumvent or adhere to the EU's stringent regulatory framework. The same cannot be said of SMEs. The prior conformity assessment can be a major obstacle to innovation and a burden that may discourage the development of AI in SMEs and startups that have limited financial and human resources. The idea of an EU presence in Digital Innovation Hubs to help them in the completion of the conformity assessment is a good one. Dedicated online tools proposed by the commission are also important to make the compliance easy to understand and to respect.

Another risk with this stringent regulation is that it may push companies to develop these AI applications out of Europe, fearing its regulation and control. It could even deprive the European market of AI-applications because of this prior assessment, like some websites that are no longer available in the EU because they do not adhere to the GDPR regulation.

EU market is broad and many companies within the EU could be competitors in the development of AI applications, hence, the commission should ensure total impartiality when assessing the conformity of the technology as well as respecting the “order of arrival” of the upcoming assessments, in order not to favor the companies of a certain country or to favor the companies that can exercise pressure on the commission to get the approval earlier or faster than another enterprise. This is more of a risk than a straight weakness - the EU has shown its boldness and detachment from lobbyists when implementing regulation before.

The EU relies on the size of its market to impose its stringent regulations. It usually assumes that the EU is sufficiently big with a strong purchasing power that firms will find it worthwhile to adhere to its regulations. When the GDPR was implemented, several websites were not accessible for EU users. Examples of those websites are LA Times, Association for National Advertisers (ANA), New York Daily News and more. They are now for the most part available as they have decided to comply with the GDPR-norm. It does not seem that many websites are still blocked due to non-compliance with GDPR. It can therefore be said that the EU was successful in its bet that firms would comply.

Can the EU allow itself to make the same gamble with AI applications? That will naturally depend on the customer group they are targeting, but in general, it can be said that EU and US customers do share many similarities. Only time will show if the EU will win its bet with AI-regulations.

Furthermore, considering the AI can learn and evolve thanks to its experience, the EU commission could define a precise time-length for which the AI application should be assessed again after a certain time of operation in order to ensure the assessments' fairness and transparency for all. The recurrence of the ex-post tests needs to be clearly defined.

As part of the mentioned online tool, the EU could develop a specific website where companies could create an account to register their AI applications. They could also apply for a conformity assessment, check its progress, and also self-test their AI systems with a check-list that would enable the companies to have automated answers and to adjust the AI system, hence sending the AI application for approval only when it appears conform to the regulation, thus preventing the commission to be overwhelmed with conformity assessments that does not meet the requirements.

5. G - VOLUNTARY LABELLING FOR NO-HIGH RISK AI APPLICATIONS

In its White Paper on AI, the Commission proposes the implementation of a voluntary labelling for no-high risk AI applications. This means that even though the application does not seem to endanger privacy and dignity of consumers or users, developers can on a voluntary basis choose to make their application certified. Once they get the labels, developers will have to meet its requirements and controls and tests will be conducted ex ante and ex post.

The use of a label can increase consumers trust. In that context we can refer to the theory of signal developed by Spence (94) in 1974. In this theory Spence explains that a signal here the label can be a good way to communicate and make someone credible. In the context of AI applications consumers or buyers are in a situation of "asymmetric information" as Akerlof explained in 1970 (95). Indeed, AI developers have much more information of their applications than people using it. A signal like a label can be a good way to reduce this information asymmetry and uncertainty and make people more willing to use the application. However, a signal can only be efficient if four conditions are checked:

A. First, the signal must be costly to implement. The more expensive the signal is, the more people will trust the application (96).

B. Developers must also show their commitment to the respect of ethics in the development of their applications (96).

C. A third party must grant the label so that consumers are sure the label is objective and credible (96).

D. The quality of the application and the respect of private life must also be easily perceived by the consumers (97).

The solution as it is currently described in the White Paper cannot be efficient. Indeed, for no-high risk AI applications, the label will not be mandatory. So, the question that is raised is the following: what will the incentive be for AI applications developers to adapt their products to the label requirements? Such adaptation is costly for developers and they will make an arbitrage between the cost of the investment and the benefits that they can draw from it. To get the label for their applications, developers will have to invest a lot of money. They will have to be very rigorous and will have to go through a lot of controls and audit. This can have consequences on the remaining part of their supply chain which will also have to adapt to these new requirements and for which this can also be too expensive. In the end, getting certified means increasing prices to make up for the costs of controls and required adaptations. That is why we think mots of no-high risk AI application developers will not change anything to get certified: the costs of it are greater than the benefits.

We can also question the efficiency of the tests conducted. Does the EU have enough money to conduct ex ante and ex post tests on a regular basis? Indeed, if these tests are not conducted regularly then the label does not make sense anymore. The label will then be seen only as a marketing tool, not as a quality signal by consumers anymore, removing therefore all benefits developers can draw from it.

5. H - GOVERNANCE

To make the governance of the AI issues efficient, the Commission proposes to create a unique structure that will govern AI. This structure will include all stakeholders from experts to consumer associations. It will not be a duplication of already existing national structures and this structure will be independent and therefore totally objective. This measure could be an efficient one and we somewhat agree with the way it will be implemented.

A possible alteration to the suggested system would be to integrate the AI-related issues within the existing European governance structure which are specialized in the different industries for three main reasons. First, it will avoid the inevitable risk of having duplicates between a horizontal governance body and sectorial governance entities. Second, it will allow the EU to adopt specific measures for each industry to take into account their specificities but also to find the right balance depending on the maturity of the industry between letting enough space for innovation and protecting the end-consumers. Third, it will make it easier to gather all the stakeholders around the table to draft the best legislation if it is done industry after industry.

References

1. **PwC.** *Sizing the prize: What's the real value of AI for your business and how can you capitalise?* s.l. : PwC, 2017.

2. **Holmes, Frank.** AI Will Add $15 Trillion To The World Economy By 2030. *forbes.com.* [Online] 2 25, 2019. https://www.forbes.com/sites/greatspeculations/2019/02/25/ai-will-add-15-trillion-to-the-world-economy-by-2030/#748e4a1852db.

3. **COMMISSION, EUROPEAN.** *Artificial Intelligence for Europe.* Brussels : EU, 2018. COM/2018/237 final.

4. **O'BRIEN, CHRIS.** AI startups raised $18.5 billion in 2019, setting new funding record. *venturebeat.com.* [Online] https://venturebeat.com/2020/01/14/ai-startups-raised-18-5-billion-in-2019-setting-new-funding-record/.

5. **OUTREACH@DARPA.MIL.** DARPA Announces $2 Billion Campaign to Develop Next Wave of AI Technologies. *darpa.mil.* [Online] https://www.darpa.mil/news-events/2018-09-07.

6. **Daniel Castro, Michael McLaughlin, Eline Chivot.** Who Is Winning the AI Race: China, the EU or the United States? *datainnovation.org.* [Online] https://www.datainnovation.org/2019/08/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/.

7. **Clement, J.** Number of monthly active Facebook users worldwide as of 1st quarter 2020. *statista.com.* [Online] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

8. **Sylvain Duranton, Jörg Erlebach, and Marc Pauly.** *Mind the (AI) Gap.* s.l. : BCG Gamma, 2018.

9. **Amiel, Sandrine.** Artificial intelligence: How is the EU planning to make up ground on US and Chinese firms? *euronews.com.* [Online] https://www.euronews.com/2020/02/19/the-eu-s-new-ai-strategy-what-you-need-to-know.

10. **Future of Life Institute.** AI POLICY – UNITED STATES. *futureoflife.org.* [Online] https://futureoflife.org/ai-policy-united-states/?cn-reloaded=1.

11. **HANNA, MINA.** Why we need to invest more in AI. *thehill.com.* [Online] https://thehill.com/opinion/technology/463120-why-we-need-to-invest-more-in-ai.

12. **DAVENPORT, THOMAS H.** China is catching up to the US on artificial intelligence research. *gcn.com.* [Online] https://gcn.com/articles/2019/02/27/china-ai-research.aspx.

13. **Pitchbook.** data on AI venture capital and private equity funding for 2016–18 for China, the European Union, and the United States. [Online] [Cited: June 7, 2019.] https://www.datainnovation.org/2019/08/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/#_edn93.

14. **Laurent Probst, Bertrand Pedersen, Virginie Lefebvre & Lauriane Dakkak-Arnoux PwC.** *Digital Transformation Monitor: USA-China-EU plans for AI: where do we stand?* s.l. : EU, 2018.

15. **Custer, C.** Report: China's government establishes $30 billion VC fund. *techinasia.com.* [Online] https://www.techinasia.com/report-chinas-government-establishes-30-billion-vc-fund.

16. **Beijing Monitoring Desk, Yawen Chen, Clarence Fernandez.** China's city of Tianjin to set up $16-billion artificial intelligence fund. *reuters.com.* [Online] https://www.reuters.com/article/us-china-ai-tianjin/chinas-city-of-tianjin-to-set-up-16-billion-artificial-intelligence-fund-idUSKCN1II0DD.

17. **Ashwin Acharya, Zachary Arnold.** *CSET Issue Brief - Chinese Public AI R&D Spending: Provisional Findings.* s.l. : CSET, 2019.

18. **Sirui, Zhou.** Giants are Pouring Money in AI - An Overview of Alibaba-Backed AI Companies. *alocean.com.* [Online] https://equalocean.com/ai/20190702-giants-are-pouring-money-in-ai-an-overview-of-alibaba-backed-ai-companies.

19. **Walch, Kathleen.** Why The Race For AI Dominance Is More Global Than You Think. *forbes.com.* [Online] https://www.forbes.com/sites/cognitiveworld/2020/02/09/why-the-race-for-ai-dominance-is-more-global-than-you-think/#15e70519121f.

20. **TSUJI, TAKASHI.** Japan to expand innovation fund to $4bn in AI push. *asia.nikkei.com.* [Online] https://asia.nikkei.com/Economy/Japan-to-expand-innovation-fund-to-4bn-in-AI-push.

21. **Craglia M. (Ed.), Annoni A., Benczur P., Bertoldi P., Delipetrev P., De Prato G., Feijoo C., Fernandez M. E., Gomez E., Iglesias M., Junklewitz H., López C. M., Martens B., Nascimento S., Nativi S., Polvora A., Sanchez I., Tolan S., Tuomi I., Vesnic A. L.** *ARTIFICIAL INTELLIGENCE, A European Perspective.* s.l. : Publications Office of the EU, 2018. ISBN 978-92-79-97219-5.

22. **Deutsches Forschungszentrum für Künstliche Intelligenz GmbH (DFKI).** AI INNOVATION COMPETITION. *German Research Center for Artificial Intelligence.* [Online] https://www.dfki.de/en/web/about-us/prizes-distinctions/ai-innovation-competition/.

23. **Center for Information and Communication Technology.** ARTIFICIAL INTELLIGENCE. *Center for Information and Communication Technology.* [Online] https://ict.fbk.eu/areas/ai/.

24. **Zubașcu, Florin.** Commission adds AI research 'lighthouse' to innovation priorities amid budget wrangle. *sciencebusiness.net.* [Online] https://sciencebusiness.net/news/commission-adds-ai-research-lighthouse-innovation-priorities-amid-budget-wrangle.

25. **CERN.** What we do. *CERN.* [Online] https://home.cern/about/what-we-do.

26. **Hoos, Prof. Dr. Holger.** CLAIRE RECEIVES BROAD MANDATE AND FUNDING FOR SHAPING "AI MADE IN EUROPE". *dfki.de.* [Online] https://www.dfki.de/en/web/news/detail/News/claire-receivesbroadmandate-ai-made-in-europe/.

27. **COLLABORATION of ELISE.** The European Commission offers significant support to Europe's AI excellence. *fcai.fi.* [Online] https://fcai.fi/news/the-european-commission-offers-significant-support-to-europes-ai-excellence.

28. **Santarsiere, Raffaella.** Digital skills shortage in Europe poses risks for the continent's future growth. *ey.com.* [Online] https://www.ey.com/en_gl/news/2018/12/digital-skills-shortage-in-europe-poses-risks-for-the-continents-future-growth.

29. **Ndemo, Bitange.** Why all children must learn code. *theconversation.com.* [Online] 12 8, 2019. https://theconversation.com/why-all-children-must-learn-code-127937.

30. **Turner, Camilla.** Teaching children coding is a waste of time, OECD chief says. *telegraph.co.uk.* [Online] 2 21, 2019. https://www.telegraph.co.uk/education/2019/02/21/teaching-children-coding-waste-time-oecd-chief-says/.

31. **World Economic Forum.** Assessing Gender Gaps in Artificial Intelligence. *reports.weforum.org.* [Online] 2018. https://reports.weforum.org/global-gender-gap-report-2018/assessing-gender-gaps-in-artificial-intelligence/.

32. **NYU Stern.** NYU Stern's Online Master of Science in Quantitative Management Program. *stern.nyu.edu.* [Online] https://www.stern.nyu.edu/programs-admissions/masters-programs/online-ms-quantitative-management/online-msqm-analytics/?utm_source=google&utm_medium=cpc&utm_campaign=nonbranded_datasci&utm_term=%2Bdata%.

33. **Google.** Google Developers Training. *developers.google.com.* [Online] https://developers.google.com/training.

34. **Knight, Will.** Why does Beijing suddenly care about AI ethics? *technologyreview.com.* [Online] 5 31, 2019. https://www.technologyreview.com/2019/05/31/135129/why-does-china-suddenly-care-about-ai-ethics-and-privacy/.

35. **Statista.** Number of small and medium-sized enterprises (SMEs) in the European Union in 2018, by size. *statista.com.* [Online] 11 2019. https://www.statista.com/statistics/878412/number-of-smes-in-europe-by-size/.

36. **Tobias Weiblen, Henry W. Chesbrough.** Engaging with Startups to Enhance Corporate Innovation. *store.hbr.org.* [Online] 3 1, 2015. https://store.hbr.org/product/engaging-with-startups-to-enhance-corporate-innovation/CMR588.

37. **European Commission.** Digital Innovation Hubs (DIHs) in Europe. *ec.europa.eu.* [Online] 5 8, 2020. https://ec.europa.eu/digital-single-market/en/digital-innovation-hubs.

38. **Jeff Loucks, Susanne Hupfer, David Jarvis, Timothy Murphy.** Future in the balance? How countries are pursuing an AI advantage. *deloitte.com.* [Online] 5 1, 2019. https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/ai-investment-by-country.html.

39. **European Comission.** The InvestEU Programme: Questions and Answers. *ec.europa.eu.* [Online] 4 18, 2019. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_2135.

40. **JONES, ELLIOT.** Will the government's new AI procurement guidelines work? *tech.newstatesman.com.* [Online] 10 3, 2019. https://tech.newstatesman.com/guest-opinion/ai-procurement-guidelines.

41. *Artificial Intelligence and the Public Sector—Applications and Challenges, International Journal of Public Administration.* **Bernd W. Wirtz, Jan C. Weyerer & Carolin Geyer.** 7, s.l. : International Journal of Public Administration, 2019, Vol. 42. https://doi.org/10.1080/01900692.2018.1498103.

42. **European Commission.** European data strategy. *ec.europa.eu.* [Online] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

43. —. Horizon Europe - the next research and innovation framework programme. *ec.europa.eu.* [Online] 2020. https://ec.europa.eu/info/horizon-europe-next-research-and-innovation-framework-programme_en.

44. —. Digital Europe Programme: a proposed €9.2 Billion of funding for 2021-2027. *ec.europa.eu.* [Online] 2019. https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu92-billion-funding-2021-2027.

45. —. EOSC Strategic Implementation Roadmap. *ec.europa.eu.* [Online] 5 2018. https://ec.europa.eu/research/openscience/pdf/eosc_strategic_implementation_roadmap_short.pdf.

46. —. Final Report and Action Plan from the European Commission Expert Group on FAIR Data: TURNING FAIR INTO REALITY. *ec.europa.eu.* [Online] 2018. https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf.

47. **Molla, Rani.** Google, Amazon and Microsoft cloud businesses helped more than double spending on data centers last year. *vox.com.* [Online] 5 15, 2018. https://www.vox.com/2018/3/15/17124300/google-amazon-microsoft-cloud-200-percent-jump-data-center-acquisitions.

48. **United Nations (UN).** United Nations Activities on Artificial Intelligence (AI). *itu.int.* [Online] 2019. https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2019-1-PDF-E.pdf.

49. **OREN ETZIONI, NICOLE DECARIO.** We have the basis for an international AI treaty. *thehill.com.* [Online] 7 17, 19. https://thehill.com/opinion/technology/452809-we-have-the-basis-for-an-international-ai-treaty.

50. **Dignum, Virginia, et al.** First Analysis of the EU Whitepaper on AI. *allai.nl.* [Online] 3 1, 2020. allai.nl/first-analysis-of-the-eu-whitepaper-on-ai/.

51. **Kahn, J.** The problem with the EU's A.I. strategy. . *Fortune.com.* [Online] 2 25, 2020. https://fortune.com/2020/02/25/eu-a-i-whitepaper-eye-on-a-i/.

52. **Niethammer, Carmen.** AI Bias Could Put Women's Lives At Risk - A Challenge For Regulators. *forbes.com.* [Online] 3 2, 2020. https://www.forbes.com/sites/carmenniethammer/2020/03/02/ai-bias-could-put-womens-lives-at-riska-challenge-for-regulators/#63135cde534f.

53. **European Parliament.** Self-driving cars in the EU: from science fiction to reality. *europarl.europa.eu.* [Online] 1 14, 2019. https://www.europarl.europa.eu/news/en/headlines/economy/20190110STO23102/self-driving-cars-in-the-eu-from-science-fiction-to-reality.

54. **EUROPEAN COMMISSION.** *Saving Lives: Boosting Car Safety in the EU.* Brussels : EUROPEAN COMMISSION, 2016. COM(2016) 787 final.

55. *Software Transparency as a Key Requirement for Self-Driving Cars.* **Cysneiros, Luiz Marcio, Raffi, Majid and Leite, Julio Cesar Sampaio do Prado.** Banff, AB, Canada : IEEE 26th International Requirements Engineering Conference, 2018. DOI: 10.1109/RE.2018.00-21.

56. *Regulation and Innovation: Evidence and Policy Implications.* **BERR – Department for Business, Enterprise and Regulatory Reform of the UK Government.** s.l. : BERR, 2008, Vol. Economics Paper No. 4.

57. **Jacques Pelkmans, Andrea Renda.** *How Can EU Legislation Enable and/or Disable Innovation.* s.l. : European Commission.

58. *The Impact of Regulation on Innovation in the United States: A Cross-Industry Literature Review.* **Stewart, Luke A.** s.l. : Information Technology & Innovation Foundation, 2010. https://itif.org/files/2011-impact-regulation-innovation.pdf.

59. **Harry Armstrong, Imre Bárd and Ebba Engström.** *REGULATOR APPROACHES TO FACILITATE, SUPPORT AND ENABLE INNOVATION.* s.l. : BEIS, 2020. BEIS Research Paper Series Number 2020/003.

60. *It runs in the family: Meta-regulation and its siblings.* **Gilad, S.** 4, s.l. : Regulation & Governance, 2010, Vol. 4. doi:10.1111/j.1748-5991.2010.01090.x..

61. *Moving beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal.* **Reyes, C. L.** 1, s.l. : Villanova Law Review, 2016, Vol. 61. Available at SSRN: https://ssrn.com/abstract=2766705.

62. **European Union.** *Liability for Artificial Intelligence and Other Emerging Technologies.* 2019.

63. *Artificial Intelligence and Legal Liability.* **Kingston, John.** s.l. : Research and Development in Intelligent Systems XXXIII: Incorporating Applications and Innovations in Intelligent Systems XXIV, 2016. DOI: 10.1007/978-3-319-47175-4_20.

64. *The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control.* **G., Hallevy.** 2, s.l. : Akron Intellectual Property Journal, 2016, Vol. 4. https://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/1.

65. **Lee Gluyas, Stefanie Day.** *Artificial Intelligence - Who is liable when AI fails to perform?* 2018.

66. *Liability Issues with Artificial Intelligence Software.* **Gerstner, M.** 1, s.l. : Santa Clara Law Review, 1993, Vol. 33.

67. **The Norwegian Data Protection Authority.** *Artificial intelligence and privacy.* s.l. : Datatilsynet, 2018.

68. **Wallace, N. and Castro, D.** *The impact of the EU's new data protection regulation on AI.* s.l. : Centre for Data Innovation: Washington, DC, USA, 2018.

69. **Timan, T. & Z. Á. Mann.** *DATA PROTECTION IN THE ERA OF ARTIFICIAL INTELLIGENCE. Trends, existing solutions and recommendations for privacy-preserving technologies.* s.l. : Big Data Value Association, 2019.

70. **Emma James, Ben Leo.** ALEXA RANT Amazon Alexa launches racist rant against Chinese government and calls coronavirus a 'terror attack'. *thesun.co.uk.* [Online] 2020. https://www.thesun.co.uk/tech/11278589/amazon-alexa-coronavirus-racist-rant/.

71. **Stupp, Catherine.** Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. *wsj.com.* [Online] 8 30, 2019. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.

72. **European Commission.** *On Artificial Intelligence - A European approach to excellence and trust.* Brussels : European Commission, 2020.

73. **Crumpler, W.** Europe's Strategy for AI Regulation. *csis.org.* [Online] 2 21, 2020. https://www.csis.org/blogs/technology-policy-blog/europes-strategy-ai-regulation.

74. **Cath-Speth, C. & Kaltheuner, F.** Risking everything: where the EU's white paper on AI falls short. *tech.newstatesman.com.* [Online] 3 3, 2020. https://tech.newstatesman.com/guest-opinion/eu-white-paper-on-artificial-intelligence-falls-short.

75. **Professional Standards Authority.** *The role of risk in regulatory policy.* s.l. : Professional Standards Authority, 2015.

76. **Daniel Castro, Eline Chivot.** How the EU Should Revise its AI White Paper Before it is Published. *datainnovation.org.* [Online] 2 1, 2020. https://www.datainnovation.org/2020/02/how-the-eu-should-revise-its-ai-white-paper-before-it-is-published/.

77. **CHASLOT, GUILLAUME.** The Toxic Potential of YouTube's Feedback Loop. *wired.com.* [Online] 7 13, 2019. https://www.wired.com/story/the-toxic-potential-of-youtubes-feedback-loop/.

78. **Venkat Atluri, Miklós Dietz, Nicolaus Henke.** Competing in a world of sectors without borders. *mckinsey.com.* [Online] McKinsey Quarterly, 7 12, 2017. https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/competing-in-a-world-of-sectors-without-borders.

79. **The New York Times.** Regulator Shopping. *nytimes.com.* [Online] 5 20, 2009. https://www.nytimes.com/2009/05/21/opinion/21thu1.html?auth=login-email&module=ArrowsNav&contentCollection=Opinion&action=keypress&region=Fixe.

80. **Feiner, Lauren.** Google cut its lobbying spending nearly in half in 2019, while Facebook took the lead. *cnbc.com.* [Online] 1 22, 2020. https://www.cnbc.com/2020/01/22/how-much-google-facebook-amazon-and-apple-spent-on-lobbying-in-2019.html.

81. **EU Debates.** *Shaping Europe's Digital Future. Ursula von der Leyen explains EU Digital Future #DigitalEU (VIDEO).* [EU Debates] s.l. : EU Debates.

82. **BOYD, AARON.** White House Tech Chief Calls Europe's AI Principles Clumsy Compared to U.S. Approach. *nextgov.com.* [Online] 2 20, 2020. https://www.nextgov.com/cio-briefing/2020/02/white-house-tech-chief-calls-europes-ai-principles-clumsy-compared-us-approach/163241/.

83. **Dastin, J.** Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters.com.* [Online] 10 10, 2018. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-airecruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G .

84. **WORLAND, JUSTIN.** Microsoft Takes Chatbot Offline After It Starts Tweeting Racist Messages. *time.com.* [Online] 3 24, 2016. https://time.com/4270684/microsoft-tay-chatbot-racism/.

85. *Manipulating machine learning: Poisoning attacks and countermeasures for regression learning.* **Jagielski, M., Oprea, B., Biggio, B., Liu, C., Nita-Rotaru, C., and Li, B.** s.l. : IEEE Symposium on Security and Privacy, 2018.

86. **HUAWEI.** *Huawei Cyber Security White Paper (Jun. 2016).* s.l. : HUAWEI, 2016.

87. **Forum, World Economic.** *White Paper: How to Prevent Discriminatory Outcomes in Machine Learning.* s.l. : World Economic Forum, 2018.

88. **Jacques Bughin, Jeongmin Seong, James Manyika, Lari Hämäläinen, Eckart Windhagen, Eric Hazan.** Tackling Europe’s gap in digital and AI. *mckinsey.com.* [Online] 2 7, 2019. https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-europes-gap-in-digital-and-ai.

89. **European Commission.** *Supporting specialised skills development: Big Data, Internet of Things and Cybersecurity for SMEs.* s.l. : European Commission, 2019. EASME/COSME/2017/007.

90. **Virginia Dignum, Catelijne Muller and Andreas Theodorou.** First Analysis of the EU Whitepaper on AI. *allai.nl.* [Online] https://allai.nl/first-analysis-of-the-eu-whitepaper-on-ai/.

91. **Reuters.** Amazon ditched AI recruiting tool that favored men for technical jobs. *theguardian.com.* [Online] 10 11, 2018. https://www.theguardian.com/technology/2018/oct/10/amazon-hiring-ai-gender-bias-recruiting-engine.

92. **Hunt, Elle.** Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter. *theguardian.com.* [Online] 3 24, 2016. https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter?CMP=twt_a-technology_b-gdntech.

93. **Vincent, James.** White House encourages hands-off approach to AI regulation. *theverge.com.* [Online] 1 7, 2020. https://www.theverge.com/2020/1/7/21054653/america-us-ai-regulation-principles-federal-agencies-ostp-principles.

94. *Market signaling: informational transfer in hiring and related screening processes.* **Spence, A-M.** Cambridge : Harvard University Press, 1974.

95. *THE MARKET FOR “LEMONS”: QUALITY UNCERTAINTY AND THE MARKET MECHANISM.* **A.AKERLOF, GEORGE.** s.l. : Academic Press: Uncertainty in Economics, 1978. https://doi.org/10.1016/B978-0-12-214850-7.50022-X.

96. *The Stock Market Reaction to the Hiring of Management Consultants: A Signalling Theory Approach.* **Donald D. Bergh, Patrick Gibbons.** 3, s.l. : Blackwell Publishing Ltd and Society for the Advancement of Management Studies: Journal of Management Studies, 2011, Vol. 48. https://doi.org/10.1111/j.1467-6486.2010.00957.x.

97. *Information and Economic Analysis: A Perspective.* **Stiglitz, Joseph E.** s.l. : Oxford University Press on behalf of the Royal Economic Society: The Economic Journal, 1985, Vol. 95. DOI: 10.2307/2232867.

98. **Deloitte China.** *Global artificial intelligence industry whitepaper .* 2019.

99. **Accenture Applied Intelligence.** Realising the Economic and Societal Potential of. *accenture.com.* [Online] 2018. https://www.accenture.com/_acnmedia/pdf-74/accenture-realising-economic-societal-potential-responsible-ai-europe.pdf.

100. *The key role of experiential uncertainty when dealing with risks: its relationships with demand for regulation and institutional trust.* **Poortvliet, P.M. and Lokhorst, A.M.** 8, s.l. : Risk Analysis, 2016, Vol. 36. DOI: 10.1111/risa.12543.

101. *Who reaps the benefits, who bears the risks? Comparative optimism, comparative utility, and regulatory preferences for mobile phone technology.* **White MP, Eiser JR, Harris PR, Pahl S.** 3, s.l. : Risk Analysis, 2007, Vol. 27. DOI: 10.1111/j.1539-6924.2007.00881.x.

102. *Perception of risk: the influence of general trust, and general confidence.* **Siegrist, M., Gutscher, H., & Earle, T. C.** 2, s.l. : Journal of risk research, 2006, Vol. 8.

103. *Delayed Privatization.* **Paolo Pinotti, Bernardo Bortolotti.** s.l. : Bank of Italy Temi di Discussione (Working Paper), 2008, Vol. 663. SSRN: https://ssrn.com/abstract=1148702.

104. *How much to trust artificial intelligence?* **Hurlburt, G.** 4, s.l. : IT Professional, 2017, Vol. 19.

105. **Marr, B.** Is Artificial Intelligence dangerous? 6 AI risks everyone should know about. *forbes.com.* [Online] 2018. https://www.forbes.com/sites/bernardmarr/2018/11/19/is-artificial-intelligence-dangerous-6-ai-risks-everyone-should-know-about/#f8e756240406.

106. *Perception of hazards: The role of social trust and knowledge.* **Siegrist, M., & Cvetkovich, G.** 5, s.l. : Risk analysis, 2000, Vol. 20.

107. *Regulations, fairness and trust.* **Lind, E. A., & Arndt, C.** s.l. : Trust and Public Policy, 2017. DOI: 10.1787/9789264268920-6-en.

108. **PricewaterhouseCoopers.** No longer science fiction, AI and robotics are transforming healthcare. *pwc.com.* [Online] 6 2017. https://www.pwc.com/gx/en/industries/healthcare/publications/ai-robotics-new-health/transforming-healthcare.html.

109. *Pedestrian trust in automated vehicles: Role of traffic signal and av driving behavior. .* **Suresh, K., Chandler, C., Dawn, M., Jessie, Y., Anuj, K., Katherine, M., & Lionel, P.** s.l. : Frontiers in Robotics and Ai, 2019. doi:10.3389/frobt.2019.00117.

110. **McCausland, P.** Self-driving Uber car that hit and killed woman did not recognize that pedestrians jaywalk. *nbcnews.com.* [Online] 11 9, 2019. https://www.nbcnews.com/tech/tech-news/self-driving-uber-car-hit-killed-woman-did-not-recognize-n1079281.

111. **Moltzau, Alex.** Artificial Intelligence Strategy for the Netherlands. *medium.com.* [Online] 1 5, 2020. https://medium.com/dataseries/artificial-intelligence-strategy-for-the-netherlands-2d5f0de2d147.

112. **European Commission.** Requirements of Trustworthy AI. *ec.europa.eu.* [Online] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/1.